Cisco Unified CallManager Express System Administrator Guide
February 2006

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100
## Contents

### Feature Map

### Preface
- Document Objectives
- Audience
- Document Organization
- Document Conventions
- Obtaining Documentation
  - Cisco.com
  - Product Documentation DVD
  - Ordering Documentation
- Documentation Feedback
- Cisco Product Security Overview
  - Reporting Security Problems in Cisco Products
- Obtaining Technical Assistance
  - Cisco Technical Support & Documentation Website
  - Submitting a Service Request
  - Definitions of Service Request Severity
- Obtaining Additional Publications and Information

### Feature History
- Feature History Overview
- Cisco ITS 1.0
- Cisco ITS 2.0
- Cisco ITS 2.01
- Cisco ITS 2.02
- Cisco ITS 2.1
- Cisco CME 3.0
- Cisco CME 3.1
- Cisco CME 3.2
- Cisco CME 3.2.1
- Cisco CME 3.2.2
Cisco CME 3.3 10
Cisco CME 3.4 10
Cisco Unified CME 4.0 10

**Cisco Unified CallManager Express Overview** 21

Cisco Unified CallManager Express Overview 21
Cisco Unified CallManager Express Network Scenarios 22
Additional Features 23
Provisioning 23
Connecting Cisco IP Phones 23

**Basic Cisco Unified CME Concepts** 24
System Design 24
Ephones 25
Ephone-dns 25
Single-Line Ephone-dn 26
Dual-Line Ephone-dn 27
Two Ephone-dns with One Number 27
Dual-Number Ephone-dn 29
Shared Ephone-dn 29
Overlaid Ephone-dn 30
Phone Number Plan 32
Direct Inward Dialing 33
PBX or Keyswitch Model 33

**Additional References** 35
Related Documents 36
Related Websites 37
Standards 37
MIBs 38
RFCs 38

**Prerequisites and Restrictions** 39
Prerequisites 39
License Prerequisites 40
Memory Prerequisites 40
Network Prerequisites 40
Restrictions 41
General Phone Support Restrictions 41
Analog Phone Support Restrictions 41
Remote SCCP Phone Support Restrictions 42
General Cisco Unified CME Restrictions 42
Installing Cisco Unified CME 43
   Installation Tasks Overview 44
   Task 1: Installing Hardware 45
   Task 2: Downloading Cisco IOS Software 46
   Task 3: Downloading Cisco Unified CME Software 46
      Cisco Unified CME Files 46
         Basic Files 47
         GUI Files 47
         Phone Firmware Files 47
         XML Template 48
         Music-on-Hold (MOH) File 48
         Script Files 48
         Bundled TSP Archive 48
      Downloading Cisco Unified CME Software 48
      Upgrading Individual Phone Firmware Files 50
   Task 4: Defining Network Settings 52
      Defining a DHCP Service 52
         Defining a Single DHCP IP Address Pool 53
         Defining a Separate DHCP IP Address Pool for Each Cisco Unified IP Phone 54
         Defining a DHCP Relay Server 56
      Changing the TFTP Server Address 57
      Setting Network Time Protocol 57
      Examples 59
      Configuring DTMF Relay for H.323 Networks 59
      Examples 60
   Task 5: Setting Cisco Unified CME Parameters 60
      Special Note About the transfer-system Command 61
      Special Parameters for Cisco Unified IP Phone 7970G and 7971G-GE 62
      Restrictions 62
      Configuring Cisco Unified CME Parameters 62
      Verifying Cisco Unified CME Parameters 68
      Examples 68
      Troubleshooting Tips 70
      Related Features 70
   Task 6: Provisioning Phones 70
      Prerequisites 71
      Provisioning Phones Using Cisco IOS Software CLI 71
      Examples 76
      Related Features 76
Task 7: Plugging in Phones 76
Task 8: Resetting and Restarting Phones 76
  Using the reset Command 77
    Examples 79
  Using the restart Command 79
    Examples 81
Task 9: Configuring Call Flows 81
Task 10: Adding Features 81
Task 11: Configuring Security for Phones 82
Task 12: Configuring Support for Multi-Site Functionality 82
Verifying the Cisco Unified CME Configuration 83
Configuration Examples 86

### Configuration File Support 91

Configuration File Support Overview 91
Externally Stored and Per-Phone Configuration Files 93
  Externally Stored and Per-Phone Configuration Files Overview 93
    Restrictions 94
  Configuring Externally Stored and Per-Phone Configuration Files 95
  Verifying Externally Stored and Per-Phone Configuration Files 96
    Examples 97
  Feature History for Externally Stored and Per-Phone Configuration Files 97
    Related Features 97
Alternative User and Network Locales 97
  Alternative User and Network Locales Overview 98
    Prerequisites 98
    Restrictions 99
  Configuring Alternative User and Network Locales 99
  Verifying Alternative User and Network Locales 102
    Examples 102
  Troubleshooting Alternative User and Network Locales 104
  Feature History for Alternative User and Network Locales 104
    Related Features 104
User-Defined User and Network Locales 105
  User-Defined User and Network Locales Overview 105
    Prerequisites 106
    Restrictions 106
  Configuring User-Defined User and Network Locales 106
  Verifying User-Defined User and Network Locales 109
Examples 110
Troubleshooting User-Defined User and Network Locales 111
Feature History for User-Defined User and Network Locales 111
Related Features 111

Dial-Plan Support 113
Dial-Plan Support Overview 113
Dial-Plan Patterns 114
  Dial-Plan Patterns Overview 114
  Configuring Dial-Plan Patterns 115
  Verifying Dial-Plan Patterns 117
  Examples 117
  Troubleshooting Dial-Plan Patterns 117
  Feature History for Dial-Plan Patterns 117
Voice Translation Rules and Profiles 117
  Voice Translation Rules and Profiles Overview 118
  Configuring Voice Translation Rules and Profiles 118
  Verifying Voice Translation Rules and Profiles 120
  Examples 121
  Troubleshooting Voice Translation Rules and Profiles 121
  Feature History for Voice Translation Rules and Profiles 121
Related Features 122

Cisco Unified CME GUI Support 123
Cisco Unified CME GUI Support Overview 123
  Prerequisites 124
  Restrictions 125
Setting Up Initial Access for the GUI Administrator 125
  Setting Up the HTTP Server 125
  Setting Up GUI Access for the System Administrator 126
Accessing the Cisco Unified CME GUI 128
Setting Up GUI Access for Customer Administrators 129
  Creating and Loading an XML Configuration File 129
  Defining a Customer Administrator 132
    Method 1: Using the Cisco Unified CME GUI to Define a Customer Administrator 132
    Method 2: Using the Cisco IOS CLI to Define a Customer Administrator 133
Setting Up GUI Access for Phone Users 134
  Method 1: Using the Cisco Unified CME GUI to Define a GUI Account for a Phone User 134
  Method 2: Using the Cisco IOS CLI to Define a GUI Account for a Phone User 135
Verifying Cisco Unified CME GUI Configuration 135
Contents

Examples 215
Verifying Transcoding Support 215
Examples 215
NM-HDV: Example 216
NM-HD and NM-HDV2: Example 216
Troubleshooting Transcoding Support 217
Verifying DSP Farm Operation 217
Tuning DSP Farm Performance 220
Feature History for Transcoding Support 221
Related Features 221

Transfer and Forwarding Support 223
Transfer and Forwarding Support Overview 223
Background 224
Strategies for Call Transfer and Call Forwarding 225
H.450.2 and H.450.3 Support 225
H.450.12 Support 228
Hairpin Call Routing 229
H.450 Tandem Gateways 231
Typical Network Scenarios for Call Transfer and Call Forwarding 233
Cisco CME 3.1 or Later and Cisco IOS Gateways 233
Cisco CME 3.1 or Later, Cisco CME 3.0 or Cisco ITS V2.1, and Cisco IOS Gateways 234
Cisco CME 3.1 or Later, Non-H.450 Gateways, and Cisco IOS Gateways 235
Cisco CME 3.1 or Later, Cisco CME 3.0 or Cisco ITS V2.1, Non-H.450 Gateways, and Cisco IOS Gateways 235
Cisco CME 3.1 or Later, Cisco Unified CallManager, and Cisco IOS Gateways 236
Cisco CME 3.1 or Later, Cisco CME 3.0 or Cisco ITS V2.1, Cisco Unified CallManager, and Cisco IOS Gateways 237

Configuring Transfer and Forwarding Support 238
Enabling or Disabling H.450.2 and H.450.3 Capabilities 240
Enabling or Disabling H.450.12 Capabilities 245
Enabling H.323-to-H.323 Connection Capabilities 248
Restrictions 248
Enabling Interworking with Cisco Unified CallManager 249
Configuring Cisco CME 3.1 or Later to Interwork with Cisco Unified CallManager 250
Configuring Cisco Unified CallManager to Interwork with Cisco CME 3.1 or Later 253
Forwarding Calls from Cisco Unified CallManager to Cisco Unity Express Using Local Hairpin Routing 254
Example 255
Setting Up Dial Peers 256
Contents

Verifying Transfer and Forwarding Support 256
Examples 256
Troubleshooting Transfer and Forwarding Support 260
Feature History for Transfer and Forwarding Support 261
Related Features 262

Trunking Support 263
Trunking Support Overview 263
Direct FXO Trunk Lines 264
  Direct FXO Trunk Lines Overview 264
  Restrictions 265
  Configuring Direct FXO Trunk Lines 266
  Verifying Direct FXO Trunk Lines 269
Examples 269
Feature History for Direct FXO Trunk Lines 270
QSIG Supplementary Services 270
  QSIG Supplementary Services Overview 270
  Configuring QSIG Supplementary Services 272
  Verifying QSIG Supplementary Services 274
Examples 274
Feature History for QSIG Supplementary Services 275
SIP Trunk Features 275
  SIP Trunk Features Overview 275
    Call Forwarding over SIP Networks 276
    Call Transfer over SIP Networks 276
    DTMF Relay 276
    SIP Register Support 277
  Configuring SIP Trunk Support 277
  Verifying SIP Trunk Support Features 280
Examples 281
Troubleshooting SIP Trunk Support Features 282
Feature History for SIP Trunk Features 283
Related Features 283

Video Support for SCCP-Based Endpoints 285
  Video Support Overview 285
    Matching Endpoint Capabilities 285
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Retrieving Video Codec Information</td>
<td>286</td>
</tr>
<tr>
<td>Call Fallback to Audio-Only</td>
<td>286</td>
</tr>
<tr>
<td>Call Setup for Video Endpoints</td>
<td>286</td>
</tr>
<tr>
<td>- Call Setup Between Two Local SCCP Endpoints</td>
<td>286</td>
</tr>
<tr>
<td>- Call Setup Between SCCP and H.323 Endpoints</td>
<td>287</td>
</tr>
<tr>
<td>- Call Setup Between Two SCCP Endpoints Across an H.323 Network</td>
<td>287</td>
</tr>
<tr>
<td>Flow of the RTP Video Stream</td>
<td>287</td>
</tr>
<tr>
<td>Prerequisites for Configuring SCCP-Based Video Endpoints</td>
<td>287</td>
</tr>
<tr>
<td>Restrictions for Configuring SCCP-Based Video Endpoints</td>
<td>288</td>
</tr>
<tr>
<td>Configuring Video for SCCP-Based Endpoints</td>
<td>289</td>
</tr>
<tr>
<td>- Configuring Slow Connect Procedures</td>
<td>290</td>
</tr>
<tr>
<td>- Enabling Video Capabilities</td>
<td>291</td>
</tr>
<tr>
<td>- Enabling Video Capabilities for a Specific Ephone</td>
<td>292</td>
</tr>
<tr>
<td>- Resetting All Ephones</td>
<td>293</td>
</tr>
<tr>
<td>- Setting Video Parameters</td>
<td>294</td>
</tr>
<tr>
<td>Verifying Video Support for SCCP-Based Endpoints</td>
<td>295</td>
</tr>
<tr>
<td>Examples</td>
<td>295</td>
</tr>
<tr>
<td>Troubleshooting Video Support for SCCP-Based Endpoints</td>
<td>296</td>
</tr>
<tr>
<td>Feature History</td>
<td>297</td>
</tr>
<tr>
<td><strong>Voice-Mail Support</strong></td>
<td>299</td>
</tr>
<tr>
<td>Voice-Mail Support Overview</td>
<td>299</td>
</tr>
<tr>
<td>Cisco Unity Express Integration</td>
<td>300</td>
</tr>
<tr>
<td>Cisco Unity Integration</td>
<td>301</td>
</tr>
<tr>
<td>DTMF Integration for Legacy Voice-Mail Applications</td>
<td>301</td>
</tr>
<tr>
<td>- DTMF Integration Overview</td>
<td>301</td>
</tr>
<tr>
<td>- Configuring DTMF Integration</td>
<td>302</td>
</tr>
<tr>
<td>- Verifying DTMF Integration</td>
<td>304</td>
</tr>
<tr>
<td>- Examples</td>
<td>304</td>
</tr>
<tr>
<td>- Feature History for DTMF Integration</td>
<td>304</td>
</tr>
<tr>
<td>Mailbox Selection Policy for Voice-Mail Servers</td>
<td>304</td>
</tr>
<tr>
<td>- Mailbox Selection Policy Overview</td>
<td>305</td>
</tr>
<tr>
<td>- Restrictions</td>
<td>305</td>
</tr>
<tr>
<td>- Configuring Mailbox Selection Policy</td>
<td>305</td>
</tr>
<tr>
<td>- Verifying Mailbox Selection Policy</td>
<td>307</td>
</tr>
<tr>
<td>- Examples</td>
<td>307</td>
</tr>
<tr>
<td>- Feature History for Mailbox Selection Policy</td>
<td>307</td>
</tr>
<tr>
<td>- Related Features</td>
<td>308</td>
</tr>
<tr>
<td>MWI Prefix Specification for SIP Voice-Mail Applications</td>
<td>308</td>
</tr>
<tr>
<td>Section</td>
<td>Page</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>SIP MWI Prefix Specification Overview</td>
<td>308</td>
</tr>
<tr>
<td>Configuring SIP MWI Prefix Specification</td>
<td>309</td>
</tr>
<tr>
<td>Verifying SIP MWI Prefix Specification</td>
<td>311</td>
</tr>
<tr>
<td>Examples</td>
<td>311</td>
</tr>
<tr>
<td>Feature History for SIP MWI Prefix Specification</td>
<td>311</td>
</tr>
<tr>
<td>Related Features</td>
<td>311</td>
</tr>
<tr>
<td>Administrative and System Features</td>
<td>313</td>
</tr>
<tr>
<td>System Features Overview</td>
<td>313</td>
</tr>
<tr>
<td>Directories</td>
<td>315</td>
</tr>
<tr>
<td>Directories Overview</td>
<td>315</td>
</tr>
<tr>
<td>Configuring Directories</td>
<td>315</td>
</tr>
<tr>
<td>Verifying Directories</td>
<td>317</td>
</tr>
<tr>
<td>Examples</td>
<td>317</td>
</tr>
<tr>
<td>Feature History for Directories</td>
<td>318</td>
</tr>
<tr>
<td>Related Features</td>
<td>318</td>
</tr>
<tr>
<td>Ephone Templates</td>
<td>318</td>
</tr>
<tr>
<td>Ephone Templates Overview</td>
<td>318</td>
</tr>
<tr>
<td>Configuring Ephone Templates</td>
<td>319</td>
</tr>
<tr>
<td>Verifying Ephone Templates</td>
<td>320</td>
</tr>
<tr>
<td>Examples</td>
<td>321</td>
</tr>
<tr>
<td>Feature History for Ephone Templates</td>
<td>321</td>
</tr>
<tr>
<td>Related Features</td>
<td>321</td>
</tr>
<tr>
<td>Ephone-dn Templates</td>
<td>322</td>
</tr>
<tr>
<td>Ephone-dn Templates Overview</td>
<td>322</td>
</tr>
<tr>
<td>Configuring Ephone-dn Templates</td>
<td>322</td>
</tr>
<tr>
<td>Verifying Ephone-dn Templates</td>
<td>323</td>
</tr>
<tr>
<td>Examples</td>
<td>324</td>
</tr>
<tr>
<td>Feature History for Ephone-dn Templates</td>
<td>324</td>
</tr>
<tr>
<td>Related Features</td>
<td>324</td>
</tr>
<tr>
<td>Feature Access Codes</td>
<td>325</td>
</tr>
<tr>
<td>Feature Access Codes Overview</td>
<td>325</td>
</tr>
<tr>
<td>Configuring Feature Access Codes</td>
<td>326</td>
</tr>
<tr>
<td>Verifying Feature Access Codes</td>
<td>328</td>
</tr>
<tr>
<td>Examples</td>
<td>328</td>
</tr>
<tr>
<td>Feature History for Feature Access Codes</td>
<td>329</td>
</tr>
<tr>
<td>Feature Control</td>
<td>329</td>
</tr>
<tr>
<td>Feature Control Overview</td>
<td>330</td>
</tr>
</tbody>
</table>
## Contents

<table>
<thead>
<tr>
<th>Feature Control</th>
<th>331</th>
</tr>
</thead>
<tbody>
<tr>
<td>Examples</td>
<td>332</td>
</tr>
<tr>
<td>Feature History for Feature Control</td>
<td>332</td>
</tr>
<tr>
<td>Related Features</td>
<td>332</td>
</tr>
<tr>
<td>Music on Hold</td>
<td>333</td>
</tr>
<tr>
<td>Music on Hold Overview</td>
<td>333</td>
</tr>
<tr>
<td>Configuring Music on Hold</td>
<td>334</td>
</tr>
<tr>
<td>Configuring Music on Hold from an Audio File</td>
<td>334</td>
</tr>
<tr>
<td>Configuring Music on Hold from a Live Feed</td>
<td>337</td>
</tr>
<tr>
<td>Verifying Music on Hold</td>
<td>341</td>
</tr>
<tr>
<td>Examples</td>
<td>341</td>
</tr>
<tr>
<td>Feature History for Music on Hold</td>
<td>342</td>
</tr>
<tr>
<td>Paging</td>
<td>342</td>
</tr>
<tr>
<td>Paging Overview</td>
<td>343</td>
</tr>
<tr>
<td>Restrictions</td>
<td>343</td>
</tr>
<tr>
<td>Configuring Paging</td>
<td>344</td>
</tr>
<tr>
<td>Verifying Paging</td>
<td>348</td>
</tr>
<tr>
<td>Examples</td>
<td>348</td>
</tr>
<tr>
<td>Feature History for Paging</td>
<td>350</td>
</tr>
<tr>
<td>Related Features</td>
<td>351</td>
</tr>
<tr>
<td>Redundant Router</td>
<td>351</td>
</tr>
<tr>
<td>Redundant Router Overview</td>
<td>351</td>
</tr>
<tr>
<td>Prerequisites</td>
<td>352</td>
</tr>
<tr>
<td>Configuring a Redundant Router</td>
<td>352</td>
</tr>
<tr>
<td>Verifying a Redundant Router</td>
<td>354</td>
</tr>
<tr>
<td>Examples</td>
<td>354</td>
</tr>
<tr>
<td>Feature History for Redundant Router</td>
<td>355</td>
</tr>
<tr>
<td>Timeouts and Tones</td>
<td>355</td>
</tr>
<tr>
<td>Timeouts and Tones Overview</td>
<td>355</td>
</tr>
<tr>
<td>Configuring Timeouts and Tones</td>
<td>356</td>
</tr>
<tr>
<td>Verifying Timeouts and Tones</td>
<td>357</td>
</tr>
<tr>
<td>Examples</td>
<td>358</td>
</tr>
<tr>
<td>Feature History for Timeouts and Tones</td>
<td>359</td>
</tr>
<tr>
<td>Related Features</td>
<td>359</td>
</tr>
<tr>
<td>XML Application Programming Interface</td>
<td>360</td>
</tr>
<tr>
<td>XML API Overview</td>
<td>360</td>
</tr>
<tr>
<td>Configuring the XML API</td>
<td>360</td>
</tr>
<tr>
<td>Configuring XML Transport Parameters</td>
<td>361</td>
</tr>
<tr>
<td>Configuring XML Application Parameters</td>
<td>362</td>
</tr>
</tbody>
</table>
Setting Authentication for XML Access 363
Setting XML Event Table Parameters 364
Verifying the XML Interface 365
Examples 366
Troubleshooting the XML Interface 366
Feature History for the XML API 367

Call-Coverage Features 369
Call-Coverage Features Overview 369

Call Forwarding 372
Call Forwarding Overview 372
Selective Call Forwarding 373
Configuring Call Forwarding 373
Verifying Call Forwarding 376
Examples 377
Troubleshooting Call Forwarding 378
Feature History for Call Forwarding 378
Related Features 379

Call Hunt 379
Call Hunt Overview 380
Ephone-dn Dial-Peer Preference 380
Huntstop 381
Configuring Call Hunt 381
Verifying Call Hunt 382
Examples 383
Troubleshooting Call Hunt 384
Feature History for Call Hunt 385
Related Features 385

Call Pickup 385
Call Pickup Overview 385
Configuring Pickup Groups 388
Verifying Call Pickup 389
Examples 390
Troubleshooting Call Pickup 390
Feature History for Call Pickup 390
Related Features 390

Call Waiting 391
Call Waiting Overview 391
Call-Waiting Beep 392
Call-Waiting Ring 392
Restrictions  393
Configuring Call Waiting  393
Verifying Call Waiting  394
Examples  395
Troubleshooting Call Waiting  395
Feature History for Call Waiting  396
Related Features  396
Cisco CME B-ACD  396
Ephone Hunt Groups  396
   Ephone Hunt Group Overview  397
      Ephone Hunt Group Basics  397
      Sequential Hunt Groups  398
      Peer Hunt Groups  399
      Longest-Idle Hunt Groups  400
      Ephone Hunt Group Agent Availability Options  401
Restrictions  405
Configuring Ephone Hunt Groups  405
Verifying Ephone Hunt Groups  411
Examples  413
Troubleshooting Ephone Hunt Groups  416
Feature History for Ephone Hunt Groups  418
Related Features  419
Night Service  420
   Night Service Overview  420
   Configuring Night Service  422
   Verifying Night Service  425
Examples  427
Troubleshooting Night-Service  428
Feature History for Night Service  428
Related Features  428
Overlaid Ephone-dns  429
   Overlaid Ephone-dns Overview  429
      Overlaid Ephone-dns Basics  429
      Call Waiting for Overlaid Ephone-dns  430
      Extending Calls for Overlaid Ephone-dns to Other Buttons on the Same Phone  432
Restrictions  432
Configuring Overlaid Ephone-dns  432
Verifying Overlaid Ephone-dns  434
Examples  435
Contents

- Callback Busy Subscriber Overview 496
- Troubleshooting Callback Busy Subscriber 497
- Feature History for Callback Busy Subscriber 497

Class of Restriction 497
- Class of Restriction Overview 498
- Configuring Class of Restriction 498
- Verifying Class of Restriction 499
- Examples 499
- Troubleshooting Class of Restriction 500
- Feature History for Class of Restriction 501
- Related Features 501

Distinctive Ringing 502
- Distinctive Ringing Overview 502
- Configuring Distinctive Ringing 502
- Verifying Distinctive Ringing 504
- Examples 504
- Feature History for Distinctive Ringing 504

Do Not Disturb 504
- Do Not Disturb Overview 505
  - Prerequisites 505
- Configuring Do Not Disturb 505
- Verifying Do Not Disturb 506
- Examples 506
- Troubleshooting Do Not Disturb 507
- Feature History for Do Not Disturb 508
- Related Features 508

Headset Auto-Answer 508
- Headset Auto-Answer Overview 509
- Configuring Headset Auto-Answer 511
- Verifying Headset Auto-Answer 512
- Examples 512
- Troubleshooting Headset Auto-Answer 513
- Feature History for Headset Auto-Answer 513

Intercom 513
- Intercom Overview 513
- Configuring Intercom 515
- Verifying Intercom 517
- Examples 518
- Feature History for Intercom 518
Cisco Unified CallManager Express System Administrator Guide

Examples 547
Feature History for Ephone-dn Labels 547

Phone Header Bar Display 547
Phone Header Bar Display Overview 548
Configuring Phone Header Bar Display 548
Verifying Phone Header Bar Display 550
Examples 550
Troubleshooting Phone Header Bar Display 550
Feature History for Phone Header Bar Display 551
Related Features 551

Soft-Key Display 551
Soft-Key Display Overview 551
Configuring Soft-Key Display 553
Verifying Soft-Key Display 555
Examples 555
Troubleshooting Soft-Key Display 556
Feature History for Soft-Key Display 557
Related Features 557

System Message Display 557
System Message Display Overview 558
Configuring System Message Display 558
Verifying System Message Display 559
Examples 560
Troubleshooting System Message Display 560
Feature History for System Message Display 561
Related Features 561

Flash Soft Key 561
Flash Soft Key Overview 561
Configuring Flash Soft Key 562
Verifying Flash Soft Key 563
Examples 563
Feature History for Flash Soft Key 563
Related Features 563

PC Port Disable 564
PC Port Disable Overview 564
Prerequisites 564
Configuring PC Port Disable 565
Verifying PC Port Disable 567
Examples 568
Troubleshooting PC Port Disable 568
Feature History for PC Port Disable 568
Related Features 569

URL Provisioning for Customized Function Buttons 569
URL Provisioning for Customized Function Buttons Overview 569
Configuring URL Provisioning for Customized Function Buttons 570
Verifying URL Provisioning for Customized Function Buttons 571
Examples 572
Troubleshooting URL Provisioning for Customized Function Buttons 572
Feature History for URL Provisioning for Customized Function Buttons 572

SRST fallback support using Cisco Unified CME 573
SRST fallback support using Cisco Unified CME Overview 573
Prerequisites 577
Restrictions 577
Configuring SRST fallback support using Cisco Unified CME 578
Specifying SRST Mode 578
Verifying SRST Mode 580
Examples 581
Prebuilding Cisco Unified CME Ephone-dn Configurations 582
Configuring Ephone-dns 583
Configuring Ephone-dn Templates and Ephone Templates for Fallback Phones 586
Configuring Telephony-Service Parameters 588
Configuring Ephone Hunt Groups 590
Examples 593
Feature History for SRST Fallback Support Using Cisco Unified CME 594
Related Features 594

Loopback Call Routing 595
Loopback Call Routing Overview 595
Configuring Loopback Call Routing 596
Verifying Loopback Call Routing 600
Examples 600
Feature History for Loopback Call Routing 600

Index 601
## Feature Map

<table>
<thead>
<tr>
<th>A</th>
<th>Call Forwarding Support 223</th>
</tr>
</thead>
<tbody>
<tr>
<td>Abbreviated Dialing Speed Dial 528</td>
<td>Call Hold 450</td>
</tr>
<tr>
<td>Account Code Entry 492</td>
<td>Call Hunt 379</td>
</tr>
<tr>
<td>Adding Directory Entries 315</td>
<td>Call Park 454</td>
</tr>
<tr>
<td>After-Hours Call Blocking 444</td>
<td>Call Pickup 385</td>
</tr>
<tr>
<td>After-Hours Toll Bar 444</td>
<td>Call Transfer 465</td>
</tr>
<tr>
<td>Agent Availability, Ephone Hunt Groups 401</td>
<td>Call Transfer Blocking 467</td>
</tr>
<tr>
<td>Agent Status Control, Ephone Hunt Groups 401</td>
<td>Call Transfer Support 223</td>
</tr>
<tr>
<td>Analog Phones 138</td>
<td>Call Waiting 391</td>
</tr>
<tr>
<td>API, XML 360</td>
<td>Call Waiting for Overlaid Ephone-dns 429</td>
</tr>
<tr>
<td>ATA (Cisco Analog Telephone Adapters) 138</td>
<td>Callback Busy Subscriber 496</td>
</tr>
<tr>
<td>Audio Paging 342</td>
<td>Called-Name Display 537</td>
</tr>
<tr>
<td>Authentication, Phone 149</td>
<td>Caller ID Blocking 475</td>
</tr>
<tr>
<td>Auto-Answer, Headset 508</td>
<td>Call-Park Blocking 458</td>
</tr>
<tr>
<td>Automatic Agent Status Not-Ready, Ephone Hunt Groups 401</td>
<td>Call-Park Redirect 458</td>
</tr>
<tr>
<td>Automatic Line Selection 493</td>
<td>Call-Waiting Beep 392</td>
</tr>
<tr>
<td>Auto-Registration Blocking 65</td>
<td>Call-Waiting Ring 392</td>
</tr>
<tr>
<td>Dedicated Call-Park Slots 456</td>
<td>Channel Huntstop 379</td>
</tr>
<tr>
<td>Dedicated FXO Trunk Lines 264</td>
<td>Cisco IP Communicator 140</td>
</tr>
<tr>
<td>DHCP Setup 52</td>
<td>Cisco VG 224 138</td>
</tr>
<tr>
<td>Dial Tone, Secondary 355</td>
<td>Class of Restriction (COR) 497</td>
</tr>
<tr>
<td>Dialing On-Hook 522</td>
<td>Conference Gain Control 481</td>
</tr>
<tr>
<td>Blocking Call Transfer 467</td>
<td>Conference Initiator Drop-Off Control 480</td>
</tr>
<tr>
<td>Blocking Caller ID 475</td>
<td>Conferencing 480</td>
</tr>
<tr>
<td>Blocking Call-Park 458</td>
<td>Configuration Files 91</td>
</tr>
<tr>
<td>Blocking Calls Based on Date and Time 444</td>
<td>Configuration Files, Externally Stored 93</td>
</tr>
<tr>
<td>Blocking Features 329</td>
<td>Configuration Files, Per-Phone 93</td>
</tr>
<tr>
<td>Blocking Local Directory 315</td>
<td>Customizing Function Buttons 569</td>
</tr>
<tr>
<td>Blocking, Automatic Registration 65</td>
<td></td>
</tr>
<tr>
<td>Bulk-Loading Speed-Dial Numbers 532</td>
<td></td>
</tr>
<tr>
<td>Busy Timeout 355</td>
<td></td>
</tr>
<tr>
<td>Call Blocking Based on Date and Time 444</td>
<td></td>
</tr>
<tr>
<td>Call Blocking Override 444</td>
<td></td>
</tr>
<tr>
<td>Call Forwarding 372</td>
<td></td>
</tr>
</tbody>
</table>
### G
- Group Call Pickup 385

### H
- Hairpin Call Routing 229
- Header Bar Display 547
- Headset Auto-Answer 508
- Hold 450
- Hold Notification 451
- Hookflash, FXO 561
- Hunt Groups, Ephone 396
- Huntstop 379
- Huntstop, Channel 379

### I
- Intercom 513
- Interdigit Timeout 355
- International Languages and Tones 62

### J
- Join Ephone Hunt Groups 401

### K
- Keep-Conference Options 481

### L
- Labels, Ephone-Dn 545
- Languages and Tones 62
- Leave Ephone Hunt Groups 401
- Line Selection for MWI 519
- Line Selection, Automatic 493
- Live-Feed Music on Hold 333
- Local Directory 315
- Local Speed Dial 525
- Locales, Alternative 97
Feature Map

Locales, User-Defined 105
Longest-Idle Ephone Hunt Groups 400
Loopback Call Routing 595

Mailbox Selection Policy 304
Monitor Mode 75
Monitor-Line Speed Dial 524
Music on Hold (MOH) 333
MWI Line Selection 519
mwi prefix command 310
MWI Prefix Specification for SIP Voice Mail 308
mwi-server command 310

Network Locales 62
Network Locales, Alternative 97
Network Locales, User-Defined 105
Network Time Protocol 57
Night Service 420
Normal Ring 75

On-hold Notification 451
On-Hook Dialing 522
Overlaid Ephone-dns 429
Overlaid Ephone-dns Call Waiting 429
Overlaid Ephone-dns Rollover Buttons 432

Paging 342
Park 454
Peer Ephone Hunt Groups 399
Per-Phone Configuration Files 93
Personal Speed Dial 527
Phone Authentication 149
Phone Display, Called-Name 537
Phone Display, Header Bar 547

Phone Display, System Message 557
Phone Function Buttons, Customizing 569
Phone Header Bar Display 547
Phone Soft-Key Display 551
Phones, Analog 138
Phones, SIP 142
Phones, Teleworker Remote 143
Pickup Groups 385
Preference, Ephone-dn Dial Peer 379

QSIG Supplementary Services 270

Secondary Dial Tone 355
Secondary Router 351
Security 149
Selective Call Forwarding 373
Sequential Ephone Hunt Groups 398
Silent Ring 75
SIP Phones 142
SIP Trunks 275
Soft-Key Display 551
Speed Dial 523
  Abbreviated Dialing 528
  Bulk Loading 532
  Local Speed Dial 525
  Monitor-Line Button 524
  Personal Speed Dial 527

Cisco Unified CallManager Express System Administrator Guide
Feature Map

Speed-Dial Buttons 528
SRST Fallback Support Using Cisco Unified CME 573
System Message Display 557

T

Tandem Gateway 231
Teleworker Remote Phones 143
Timeout, Busy 355
Timeout, Interdigit 355
Timeout, Ringing 355
Toll Bar and Toll Bar Override 444
Tone, Secondary Dial 355
Transcoding Support 199
Transfer 465
Transfer Support 223
Translation Profiles 117
Translation Rules 117
Trunking Support 263
Trunks, SIP 275

U

URL Provisioning for Customized Function Buttons 569
User Locales 62
User Locales, Alternative 97
User-Defined User and Network Locales 105

V

Video Support 285
Voice Mail Integration 299
Voice Translation Profiles 117
Voice Translation Rules 117

X

XML Application Programming Interface 360
XML Configuration Files 91
Preface

Revised: February 2006

This chapter describes the objectives, audience, organization, and conventions used in the Cisco Unified CallManager Express System Administrator Guide. It also provides sources for obtaining documentation, technical assistance, and additional publications and information from Cisco Systems. It contains the following sections:

- Document Objectives
- Audience
- Document Organization
- Document Conventions
- Obtaining Documentation
- Documentation Feedback
- Cisco Product Security Overview
- Obtaining Technical Assistance
- Obtaining Additional Publications and Information

**Document Objectives**

This document describes features and tasks associated with Cisco Unified CallManager Express (Cisco Unified CME).
Audience

This document is intended primarily for system administrators who configure and maintain Cisco Unified CME but who may not be familiar with the tasks, the relationship between tasks, or the Cisco IOS software commands necessary to perform particular tasks. This configuration guide is also intended for expert users experienced with Cisco Unified CME who need to know about new features, new configuration options, and new software characteristics in the current Cisco IOS software release.

System administrators who are setting up a Cisco Unified CME system should be familiar with the following:

- TCP/IP fundamentals: IP addressing, routing, DHCP, HTTP, NTP, TFTP.
- Cisco IOS fundamentals: command-line interface (CLI) operation, VLAN configuration, and flash memory and TFTP file management.
- VoIP fundamentals: configuring and verifying dial peers and voice ports.

Document Organization

This document contains the sections described in Table 1.

<table>
<thead>
<tr>
<th>Section Title</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Feature Map</td>
<td>Alphabetically organized links to Cisco Unified CME features.</td>
</tr>
<tr>
<td>Feature History</td>
<td>Detailed history of the features in each Cisco Unified CME release.</td>
</tr>
<tr>
<td>Cisco Unified CallManager Express Overview</td>
<td>High-level descriptions of Cisco Unified CME basic concepts.</td>
</tr>
<tr>
<td>Prerequisites and Restrictions</td>
<td>Prerequisites and restrictions associated with Cisco Unified CME.</td>
</tr>
<tr>
<td>Installing Cisco Unified CME</td>
<td>Step-by-step instructions for installing Cisco Unified CME.</td>
</tr>
<tr>
<td>Configuration File Support</td>
<td>Externally stored and per-phone configuration files, alternative and user-defined user locales and network locales.</td>
</tr>
<tr>
<td>Dial-Plan Support</td>
<td>Dial-plan patterns and voice translation rules and profiles.</td>
</tr>
<tr>
<td>Cisco Unified CME GUI Support</td>
<td>Graphical user interface allows you to provision Cisco Unified CME phones and features.</td>
</tr>
<tr>
<td>Phone Support</td>
<td>Analog phones, Cisco IP Communicator, and teleworker remote phones.</td>
</tr>
<tr>
<td>Phone Authentication</td>
<td>Secure SCCP signaling between Cisco Unified CME and Cisco Unified IP phones.</td>
</tr>
<tr>
<td>Transcoding Support</td>
<td>Resources for converting packets from one codec to another.</td>
</tr>
</tbody>
</table>
Table 1  Cisco Unified CallManager Express System Administrator Guide Document Organization

<table>
<thead>
<tr>
<th>Section Title</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transfer and Forwarding Support</td>
<td>Options for interworking with networks and other systems.</td>
</tr>
<tr>
<td>Trunking Support</td>
<td>Direct FXO lines, QSIG supplementary services, and SIP trunks.</td>
</tr>
<tr>
<td>Video Support for SCCP-Based Endpoints</td>
<td>Support for video transmission between two video-capable SCCP endpoints or between SCCP and H.323 endpoints</td>
</tr>
<tr>
<td>Voice-Mail Support</td>
<td>Commands for interworking with voice-mail systems.</td>
</tr>
<tr>
<td>Administrative and System Features</td>
<td>Directories, ephone templates, ephone-dn templates, feature access codes, feature control, music on hold, paging, and timeouts and tones.</td>
</tr>
<tr>
<td>Call-Coverage Features</td>
<td>Call forwarding, call hunt, call pickup, call waiting, ephone hunt groups, night service, and overlaid ephone-dns.</td>
</tr>
<tr>
<td>Call-Handling Features</td>
<td>Call blocking based on date and time (after-hours toll bar), call hold, call park, call transfer, caller ID blocking, and conferencing.</td>
</tr>
<tr>
<td>Phone Features</td>
<td>Features related to phone answering and dialing (such as headset auto-answer and speed dial), phone displays (such as soft-key display), and phone functions (such as PC port disable and custom function buttons).</td>
</tr>
<tr>
<td>SRST fallback support using Cisco Unified CME</td>
<td>SRST fallback support for Cisco Unified CallManager phones using Cisco Unified CME on a gateway router.</td>
</tr>
<tr>
<td>Loopback Call Routing</td>
<td>Software-based limited emulation of back-to-back physical voice ports.</td>
</tr>
<tr>
<td>Index</td>
<td>—</td>
</tr>
</tbody>
</table>

Document Conventions

Within Cisco IOS software documentation, the term *router* is generally used to refer to a variety of Cisco products (for example, routers, access servers, and switches). Routers, access servers, and other networking devices that support Cisco IOS software are shown interchangeably within examples. These products are used only for illustrative purposes; that is, an example that shows one product does not necessarily indicate that other products are not supported.
The Cisco IOS documentation set uses the following conventions:

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>^ or Ctrl</td>
<td>The ^ and Ctrl symbols represent the Control key. For example, the key combination ^D or Ctrl-D means hold down the Control key while you press the D key. Keys are indicated in capital letters but are not case sensitive.</td>
</tr>
<tr>
<td>string</td>
<td>A string is a nonquoted set of characters shown in italics. For example, when setting an SNMP community string to public, do not use quotation marks around the string or the string will include the quotation marks.</td>
</tr>
</tbody>
</table>

Command syntax descriptions use the following conventions:

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>boldface</td>
<td>Boldface text indicates commands and keywords that you enter literally as shown.</td>
</tr>
<tr>
<td>italics</td>
<td>Italic text indicates arguments for which you supply values.</td>
</tr>
<tr>
<td>[x]</td>
<td>Square brackets enclose an optional element (keyword or argument).</td>
</tr>
<tr>
<td>[x</td>
<td>y]</td>
</tr>
<tr>
<td>{x</td>
<td>y}</td>
</tr>
<tr>
<td>{x [y</td>
<td>z]}</td>
</tr>
</tbody>
</table>

Nested sets of square brackets or braces indicate optional or required choices within optional or required elements. For example:

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>[x {y</td>
<td>z}]</td>
</tr>
</tbody>
</table>

Examples use the following conventions:

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>screen</td>
<td>Examples of information displayed on the screen are set in Courier font.</td>
</tr>
<tr>
<td>boldface screen</td>
<td>Examples of text that you must enter are set in Courier bold font.</td>
</tr>
<tr>
<td>&lt; &gt;</td>
<td>Angle brackets enclose text that is not printed to the screen, such as passwords.</td>
</tr>
<tr>
<td>!</td>
<td>An exclamation point at the beginning of a line indicates a comment line. (Exclamation points are also displayed by the Cisco IOS software for certain processes.)</td>
</tr>
<tr>
<td>[ ]</td>
<td>Square brackets enclose default responses to system prompts.</td>
</tr>
</tbody>
</table>

The following conventions are used to attract the attention of the reader:

**Caution**

Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.
Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:
http://www.cisco.com/techsupport

You can access the Cisco website at this URL:
http://www.cisco.com

You can access international Cisco websites at this URL:

Product Documentation DVD

The Product Documentation DVD is a comprehensive library of technical product documentation on a portable medium. The DVD enables you to access multiple versions of installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the same HTML documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .PDF versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at this URL:
http://www.cisco.com/go/marketplace/

Ordering Documentation

Registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:
http://www.cisco.com/go/marketplace/
You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can submit comments about Cisco documentation by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems  
Attn: Customer Document Ordering  
170 West Tasman Drive  
San Jose, CA 95134-9883  
We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:


From this site, you will find information about how to:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories, security notices, and security responses for Cisco products is available at this URL:

http://www.cisco.com/go/psirt

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at this URL:


Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you have identified a vulnerability in a Cisco product, contact PSIRT:

- For Emergencies only—security-alert@cisco.com

An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.
For Nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:
- 1 877 228-7302
- 1 408 525-6532

Tip
We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.x through 9.x.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:


The link on this page has the current PGP key ID in use.

If you do not have or use PGP, contact PSIRT at the aforementioned e-mail addresses or phone numbers before sending any sensitive material to find other means of encrypting the data.

Obtaining Technical Assistance
Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website
The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:


Note
Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the Tools & Resources link under Documentation & Tools. Choose Cisco Product Identification Tool from the Alphabetical Index drop-down list, or click the Cisco Product Identification Tool link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting show command
output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

**Submitting a Service Request**

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests, or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

**Definitions of Service Request Severity**

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—An existing network is down, or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of the network is impaired, while most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.
Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco offerings. To order and find out more about the Cisco Product Quick Reference Guide, go to this URL:
  
  http://www.cisco.com/go/guide

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

  http://www.cisco.com/go/marketplace/

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

  http://www.cisco.com/go/iqmagazine

  or view the digital edition at this URL:

  http://ciscoiq.texterity.com/ciscoiq/sample/

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/ipj

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:


- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

  http://www.cisco.com/discuss/networking
- World-class networking training is available from Cisco. You can view current offerings at this URL:
Feature History

Cisco Unified CallManager Express (Cisco Unified CME) is a call-processing application in Cisco IOS software that enables Cisco routers to deliver key-system or hybrid PBX functionality for enterprise branch offices or small businesses. This chapter contains the following sections:

- Feature History Overview, page 2
- Cisco ITS 1.0, page 3
- Cisco ITS 2.0, page 4
- Cisco ITS 2.01, page 5
- Cisco ITS 2.02, page 5
- Cisco ITS 2.1, page 5
- Cisco CME 3.0, page 6
- Cisco CME 3.1, page 7
- Cisco CME 3.2, page 8
- Cisco CME 3.2.1, page 9
- Cisco CME 3.2.2, page 9
- Cisco CME 3.3, page 10
- Cisco CME 3.4, page 10
- Cisco Unified CME 4.0, page 10

Note Prior to version 4.0, the name of this product was Cisco CallManager Express (Cisco CME). Prior to version 3.0, the name was Cisco IOS Telephony Services (Cisco ITS).

Feature History Overview

This chapter lists the features found in different Cisco Unified CME software releases. Other support information is available through the following links:

- Finding Support Information for Platforms and Cisco IOS Software Images, page 2
- Finding Support Information for Cisco Unified CME, page 2

Finding Support Information for Platforms and Cisco IOS Software Images
Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click Cancel at the login dialog box and follow the instructions that appear.

Finding Support Information for Cisco Unified CME
Each Cisco Unified CME release has a specifications document called Supported Firmware, Platforms, Memory, and Voice Products, which lists release-specific information such as the maximum number of phones, memory requirements, supported phone firmware files, and compatible voice products. Locate this document for your particular release at the Cisco Unified CME Documentation Roadmap at http://www.cisco.com/en/US/products/sw/voicesw/ps4625/products_documentation_roadmap09186a080189132.html.
## Cisco ITS 1.0

### Table 2  Cisco ITS 1.0 Features

<table>
<thead>
<tr>
<th>Cisco IOS Release</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.1(5)YD</td>
<td>Cisco IOS Telephony Services was introduced on the Cisco 2600 series, Cisco 3600 series, and Cisco IAD2420 series.</td>
</tr>
<tr>
<td></td>
<td>- Support for Cisco IP Phone 7910, Cisco IP Phone 7940, and Cisco IP Phone 7960</td>
</tr>
<tr>
<td></td>
<td>- Multiple lines per Cisco IP phone</td>
</tr>
<tr>
<td></td>
<td>- Multiple shared-line appearances across phones</td>
</tr>
<tr>
<td></td>
<td>- Call forwarding for all calls or for busy and no-answer conditions</td>
</tr>
<tr>
<td></td>
<td>- Call transfer</td>
</tr>
<tr>
<td></td>
<td>- Distinctive ringing for external and internal calls</td>
</tr>
<tr>
<td></td>
<td>- Dial-plan class of restriction (COR)</td>
</tr>
<tr>
<td></td>
<td>- Call hold and retrieve</td>
</tr>
<tr>
<td></td>
<td>- Call pickup of on-hold calls</td>
</tr>
<tr>
<td></td>
<td>- Caller identification display and blocking</td>
</tr>
<tr>
<td></td>
<td>- Function keys</td>
</tr>
<tr>
<td></td>
<td>- Speed dialing</td>
</tr>
<tr>
<td></td>
<td>- Cisco IP phones derive the date and time from the router through Network Time Protocol (NTP)</td>
</tr>
<tr>
<td></td>
<td>- Interworking with Cisco gatekeeper</td>
</tr>
<tr>
<td></td>
<td>- Analog foreign exchange station (FXS) and foreign exchange office (FXO) ports</td>
</tr>
<tr>
<td></td>
<td>- On-net calls using Voice over IP (VoIP) H.323, Voice over Frame Relay (VoFR), and Voice over ATM (VoATM)</td>
</tr>
</tbody>
</table>
## Cisco ITS 2.0

### Table 3  Cisco ITS 2.0 Features

<table>
<thead>
<tr>
<th>Cisco IOS Release</th>
<th>Description</th>
</tr>
</thead>
</table>
| 12.2(2)XT         | This service was implemented on the Cisco 1750 and Cisco 1751.  
|                   | - Cisco IP Conference Station 7935 support  
|                   | - Two-call support for Cisco IP Phone 7910  
|                   | - Three-party conference (G.711 calls)  
|                   | - Intercom for Cisco IP phones  
|                   | - Paging for Cisco IP phones and for external system  
|                   | - Call transfers across an H.323 network  
|                   | - Music on hold (MOH)  
|                   | - Graphical user interface (GUI) using a standard web browser  
|                   | - Recent call history and activity display  
|                   | - Call forwarding enhancements (huntstop)  
|                   | - Digit manipulation using translation rules  
|                   | - Enhancements to distinctive ringing for internal and external calls  
|                   | - Cisco Unity voice-mail integration including message-waiting indication  
|                   | - On-hold call timeout alert  
|                   | - Session Initiation Protocol (SIP) unsolicited message-waiting notification support  
|                   | - Local phone directory display and search on Cisco IP phone  
|                   | - XML services support on Cisco IP phones  
|                   | - Basic Telephony Application Programming Interface (TAPI)-aware PC application support  
|                   | - Interactive voice response (IVR) and auto-attendant support using Tool Command Language (Tcl)  
| 12.2(8)T          | This service was integrated into Cisco IOS Release 12.2(8)T and implemented on the Cisco 3725 and Cisco 3745.  
| 12.2(8)T1         | This service was implemented on the Cisco 2600XM and Cisco 2691.  

## Cisco ITS 2.01

### Table 4  Cisco ITS 2.01 Features

<table>
<thead>
<tr>
<th>Cisco IOS Release</th>
<th>Description</th>
</tr>
</thead>
</table>
| 12.2(11)T         | • This service was implemented on the Cisco 1760, and support for Cisco 1750 was removed.  
|                   | • Support was added for an increased number of directory numbers or virtual voice ports on Cisco IP phones.  
|                   | • Support was added for ATA-186.  
|                   | • Support was added for top-line display description on the Cisco IP Phones 7940 and 7940G and the Cisco IP Phones 7960 and 7960G. |

## Cisco ITS 2.02

### Table 5  Cisco ITS 2.02 Features

<table>
<thead>
<tr>
<th>Cisco IOS Release</th>
<th>Description</th>
</tr>
</thead>
</table>
| 12.2(13)T         | • This service was implemented on the Cisco Catalyst 4000 family, Cisco Catalyst 4224, and Cisco 3640A. Support was removed for the Cisco 2610, Cisco 2611, Cisco 2620, Cisco 2621, and Cisco 3620.  
|                   | • Support was added for an increased number of directory numbers or virtual voice ports on Cisco IP phones. |

## Cisco ITS 2.1

### Table 6  Cisco ITS 2.1 Features

<table>
<thead>
<tr>
<th>Cisco IOS Release</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(11)YT1</td>
<td>The <code>reset</code> command was modified and the <code>restart</code> command was introduced to provide more options when IP phones are rebooted after configuration updates.</td>
</tr>
<tr>
<td>12.2(15)T</td>
<td>ITS Version 2.1 was integrated into Cisco IOS Release 12.2(15)T.</td>
</tr>
</tbody>
</table>
Table 7 Cisco ITS 3.0 Features

<table>
<thead>
<tr>
<th>Cisco IOS Release</th>
<th>Description</th>
</tr>
</thead>
</table>
| 12.2(15)ZJ        | This service was implemented on the Cisco 3640A and the Cisco IAD2430 series. Support was added for the following features:  
  - ITS setup tool for quick installation  
  - Automatic assignment of free extension numbers to new IP phones  
  - Night service  
  - Call blocking (toll bar) based on time of day, day of week, or date  
  - Call blocking (toll bar) override  
  - Call pickup and call-pickup groups  
  - Hunt groups  
  - Secondary dial tone  
  - Three types of speed dial: speed-dial buttons, local speed-dial numbers common to all users, and personal speed-dial numbers that can be updated by an administrator or from the phone.  
  - Cisco IP Phone 7902G, Cisco IP Phone 7905G, Cisco IP Phone 7912G  
  - Account code entry  
  - Callback busy subscriber  
  - Do not disturb  
  - International date format, language, and call-progress tone support  
  - Call-forward-all soft key on Cisco IP phones  
  - Flash soft key for hookflash functionality for the public switched telephone network (PSTN)  
  - Dual-line mode to support call waiting and other features  
  - Extension overlays for better call handling and distribution  
  - Fast-dial support  
  - GUI enhancements  
  - Label support  
  - Busy lamp monitor and direct station select  
  - Phone directory entry  
  - Silent and feature ring options |

12.2(15)ZJ1 The name keyword was added to the clid strip command.
**Table 7  Cisco ITS 3.0 Features (Continued)**

<table>
<thead>
<tr>
<th>Cisco IOS Release</th>
<th>Description</th>
</tr>
</thead>
</table>
| 12.2(15)ZJ3       | - The product name was changed from Cisco IOS Telephony Services (Cisco ITS) to Cisco CallManager Express (Cisco CME).  
- Support was added for an increased number of directory numbers or virtual voice ports on Cisco IP phones.  
- Limited support was provided for the Cisco Wireless IP Phone 7920 in 7960-emulation mode.  
- Local hairpin call routing was supported as an option for networks that cannot support H.450 call transfer and forwarding. This feature requires installation of the Tcl script app_h450_transfer.2.0.0.8.tcl or a later version. |

| 12.3(4)T          | Cisco CME 3.0 was integrated into Cisco IOS Release 12.3(4)T. |
| 12.2(15)ZJ4       | The secondary keyword was added to the calling-number local command. |

**Cisco CME 3.1**

**Table 8  Cisco CME 3.1 Features**

<table>
<thead>
<tr>
<th>Cisco IOS Release</th>
<th>Description</th>
</tr>
</thead>
</table>
| 12.3(7)T          | - Basic call handling, call transfer, and call forwarding—Enhancements for VoIP networks containing a mix of platforms that support H.450.2 and H.450.3 standards, such as Cisco CME 3.1, Cisco CME 3.0, and Cisco ITS V2.1, and platforms that do not support H.450.2 and H.450.3 standards, such as Cisco CallManager, Cisco BTS Softswitch (BTS), and Cisco PSTN Gateway (PGW).  
  - Support for H.450.12 standards.  
  - Automatic detection of Cisco CallManager endpoints.  
  - Hairpin VoIP-to-VoIP call routing and routing to an H.450 tandem gateway.  
- Call park allows calls to be commonly held and retrieved by anyone.  
- Automatic line selection enhancement specifies a particular button as the line automatically used for outgoing calls.  
- CFwdAll soft key restriction control restricts the number of digits that can be entered using the CFwdAll soft key.  
- Ephone-hunt group enhancements allows secondary numbers for pilot numbers.  
- Language display localization and directory search are supported on Cisco IP Phone 7905G and Cisco IP Phone 7912G. Call progress tone localization is supported on Cisco IP Phone 7902G, Cisco IP Phone 7905G, and Cisco IP Phone 7912G.  
- The Cisco Wireless IP Phone 7920 and Cisco IP Conference Station 7936 are fully supported in the Cisco IOS command-line interface (CLI) and Cisco CME GUI. The Cisco Wireless IP Phone 7920 internally supports display translation to French and German from English. |
## Table 9  Cisco CME 3.2 Features

<table>
<thead>
<tr>
<th>Cisco IOS Release</th>
<th>Description</th>
</tr>
</thead>
</table>
| 12.3(11)T         | Network features  
  - Transcoding between G.711 and G.729; see the “Transcoding Support” section on page 199.  
  - H.323-to-SIP call routing to Cisco Unity Express; see Integrating Cisco CallManager Express with Cisco Unity Express  
  - DTMF relay enhancement for SIP calls; see the “SIP Trunk Features” section on page 275.  
| Phone features |  
  - Customization of soft-key display; see the “Soft-Key Display” section on page 551.  
| Call center features |  
  - Dynamic hunt group login and logout; see the “Do Not Disturb” section on page 504.  
  - Addition of the statistics and statistics last keywords to the show ephone-hunt command; see show ephone hunt in the Cisco Unified CallManager Express Command Reference.  
  - Addition of the longest-idle keywork to the ephone-hunt command; see the “Ephone Hunt Groups” section on page 396.  
| System features |  
  - Call-waiting beep customization; see the “Call Waiting” section on page 391.  
  - Called name display for overlay ephone-dns and dialed number identification service (DNIS) calls; see the “Called-Name Display” section on page 537.  
  - IP phones display the original calling parties’ IDs automatically.  
  - Conference initiator drop-off control; see the “Conferencing” section on page 480.  
  - Consult transfer support for direct station; see the “Call Transfer” section on page 465.  
  - Direct FXO trunk line support; see the “Direct FXO Trunk Lines” section on page 264.  
  - Immediate call forward to voice mail or other call-forward no answer (CFNA) target numbers; see the “Do Not Disturb” section on page 504.  
  - When a local IP phone calls another local IP phone that is in the do not disturb (DND) state, the message “Ring out DND” is displayed on the calling phone, indicating that the target phone is in the DND state.  
  - Monitor-line button speed dial; see the “Speed Dial” section on page 523  
  - Night service call notification is sent automatically every 12 seconds until the call is either answered or aborted.  
  - Translation profile support for ephone-dn; see the “Voice Translation Rules and Profiles” section on page 117.  

Cisco CME 3.2.1

Table 10  Cisco CME 3.2.1 Features

<table>
<thead>
<tr>
<th>Cisco IOS Release</th>
<th>Description</th>
</tr>
</thead>
</table>
| 12.3(11)XL        | • Basic automatic call distribution (B-ACD) and auto attendant (AA) service is available to provide the following:  
|                   |   – A menu for outside callers with options that allow one-key dialing and extension-number access  
|                   |   – Call queuing  
|                   |   – Tools for obtaining call statistics  
|                   | See the “Configuring an Attendant for Primary Call Coverage” chapter in the Cisco CME 3.2 System Administration Guide.  
|                   | • The Cisco IP Phone 7970G is supported.  
|                   | • Call Waiting for overlaid ephone-dns. See the “Overlaid Ephone-dns” section on page 429.  
|                   | • Ringing for call-waiting notification per ephone-dn. See the “Call Waiting” section on page 391.  
|                   | • Do not disturb (DND) can be blocked from phones. See the “Do Not Disturb” section on page 504.  
|                   | • An ephone-dn of an ephone hunt group can be configured to go into not-ready status automatically after a call to the ephone-dn is unanswered. See the “Ephone Hunt Group Agent Availability Options” section on page 401. |

Cisco CME 3.2.2

Table 11  Cisco CME 3.2.2 Features

<table>
<thead>
<tr>
<th>Cisco IOS Release</th>
<th>Description</th>
</tr>
</thead>
</table>
| 12.3(11)XL1       | • The Cisco IP Phone 7971G-GE is supported.  
|                   | • A conference gain control for external calls has been added. See the “Conferencing” section on page 480.  
|                   | • An intercom no-mute function has been added. See the “Intercom” section on page 513.  
|                   | • Call-park slot status can be observed using monitor mode. See the “Call Park” section on page 454. |
Cisco CME 3.3

Table 12  Cisco CME 3.3 Features

<table>
<thead>
<tr>
<th>Cisco IOS Release</th>
<th>Description</th>
</tr>
</thead>
</table>
| 12.3(14)T         | • Cisco CME B-ACD has a new mode called drop-through mode, in which incoming calls to the B-ACD AA are put directly through to an agent without encountering an interactive menu. Cisco CME B-ACD now supports multiple AA applications per Cisco CME system.  

**Note**  For more information, see *Cisco Unified CME B-ACD and Tcl Call-Handling Applications*.  
• The maximum number of members in an ephone-hunt group was increased to 20.  
• The maximum number of ephone-dns that can be overlaid on a single button was increased to 25.

Cisco CME 3.4

Table 13  Cisco CME 3.4 Features

<table>
<thead>
<tr>
<th>Cisco IOS Release</th>
<th>Description</th>
</tr>
</thead>
</table>

Cisco Unified CME 4.0

With this release, the product name has been changed to Cisco Unified CallManager Express (Cisco Unified CME). Enhancements were introduced in the following areas:  
• Basic Automatic Call Distribution (B-ACD) and Auto-Attendant (AA) Service  
• Direct Inward Dial Digit Translation Service  
• Call Forwarding  
• Call Park  
• Call Transfer  
• Conference  
• Ephone Hunt Groups  
• Ephone Templates and Ephone-dn Templates  
• Phone Features  
• Phone Support  
• Security Features  
• User Features  
• Video Support  
• Administrative Features
### Table 14  Cisco Unified CME 4.0 Features

<table>
<thead>
<tr>
<th>Cisco IOS Release</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Basic Automatic Call Distribution (B-ACD) and Auto-Attendant (AA) Service</strong></td>
<td></td>
</tr>
</tbody>
</table>
| 12.4(4)XC | Drop-through mode—Incoming calls to the B-ACD AA are put directly through to an agent if no greeting is configured. If all agents are busy, callers are put in queue and hear MOH until an agent is free. If a greeting is configured, callers hear the greeting and then are put through to an agent or the queue.  
  [See Cisco Unified CME B-ACD and Tcl Call-Handling Applications.](#) |
| 12.4(4)XC | Increased maximum number of auto-attendant applications—Up to three AA applications can be set up per Cisco Unified CME system, and each application can be set up differently. All the AAs feed calls to a single call-queue application that distributes the calls. A total of ten hunt groups (call queues) can be configured for the call-queue application, with three hunt groups for each AA and the tenth group acting as a shared operator-hunt-group. Hunt groups can be shared among AAs or dedicated to specific AAs.  
  [See Cisco Unified CME B-ACD and Tcl Call-Handling Applications.](#) |
| 12.4(4)XC | Improved waiting call notification—When a call is waiting in a call queue, the phone users who are members of the queue’s hunt group are notified by call-waiting beep, text display, and lit message lamp.  
  No special configuration is required. |
| 12.4(4)XC | Music on hold from a live feed—Calls that are on hold in the B-ACD call queue can hear music on hold from a live feed. The music-on-hold live feed must be configured as described in the “Music on Hold” section on page 333.  
  No special configuration is required. |
| 12.4(4)XC | Call coverage when all hunt-group agents are in not-ready status—To forward calls when all members of a hunt group are unavailable, use the **param voice-mail** command to specify an alternate destination number that you have set up to provide coverage. Although the command name contains the term “voice-mail,” the command can be used to direct calls to any arbitrary extension number. For example, you can use this command to direct calls to a night-bell device or central answering point.  
  The **display-logout** command can then be used to display a message on the phones of hunt-group agents to notify them that the alternate destination call routing for B-ACD hunt-group calls is active.  
  For more information, see [Cisco Unified CME B-ACD and Tcl Call-Handling Applications](#).  
  Use the **param voice-mail** command to specify an alternate destination number that is set up to provide coverage for B-ACD hunt-group calls.  
  Use the **display-logout** command to specify a message for display on hunt-group phones. |
| 12.4(4)XC | Call-hold statistics added to reports—New fields describing the amount of time that calls spend in the hold state have been added to the statistical reports for Cisco Unified CME B-ACD applications.  
  For more information, see the **show ephone-hunt** and the **hunt-group report url** command reference entries.  
  No special configuration is required. |
| 12.4(4)XC | The **ephone-hunt statistics write-all** command writes out in hourly increments all the ephone hunt group statistics for the past seven days. This command is intended be used when normal hunt group statistics collection is interrupted, perhaps due to TFTP server failure.  
  [See Cisco Unified CME B-ACD and Tcl Call-Handling Applications.](#) |
### Direct Inward Dial Digit Translation Service

<table>
<thead>
<tr>
<th>Cisco IOS Release</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(4)XC</td>
<td><strong>Direct Inward Dial (DID) Digit Translation Service</strong>—A Tcl script provides number transformation for DID calls when the range of DID numbers provided by the PSTN Central Office (CO) does not match the range of Cisco Unified CME extension numbers in the internal dial plan. See <em>Cisco Unified CME B-ACD and Tcl Call-Handling Applications</em>.</td>
</tr>
</tbody>
</table>

### Call Forwarding

<table>
<thead>
<tr>
<th>Cisco IOS Release</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(4)XC</td>
<td><strong>Automatic call forwarding during night service</strong>—Ephone-dns (extensions) can be designated to automatically forward their calls to a specified number during the time that night service is in effect. See Call Forwarding, page 372.</td>
</tr>
<tr>
<td>12.4(4)XC</td>
<td><strong>Selective call forwarding</strong>—Call forwarding for busy and no-answer ephone-dns can be applied selectively based on the number that a caller dials for a particular ephone-dn: the primary number, the secondary number, or either of those numbers expanded through the use of a dial-plan pattern. See Call Forwarding, page 372.</td>
</tr>
</tbody>
</table>

### Call Park

<table>
<thead>
<tr>
<th>Cisco IOS Release</th>
<th>Description</th>
</tr>
</thead>
</table>
| 12.4(4)XC         | **Dedicated call-park slots**—A private call-park slot can be configured for each ephone. Every line on the phone can use the slot, but only one call can be parked at any time. Optional parameters include timeout intervals, after which the parked call can be automatically recalled to the parking phone or transferred to another number. If a phone is configured with a private park slot, its user can park a call by pressing the following keys:  
  - IP phone—Park soft key or Transfer soft key, then the FAC for call park.  
  - Analog phone—Hookflash, then the FAC for call park. See Call Park, page 454. |
| 12.4(4)XC         | **Call park blocked per ephone**—Individual ephones can be blocked from parking calls at call-park slots. If a blocked ephone has a dedicated park slot, it will still be able to park calls at the dedicated park slot, but not at any other park slot. See Call Park, page 454. |
| 12.4(4)XC         | **Call park redirect**—The call-park system redirect command allows you to specify that H.323 and SIP calls should use H.450 or the SIP Refer method of call forwarding or transfer to park calls and to pick up calls from park. The default if this command is not used is that hairpin call forwarding or transfer is used to park calls and to pick up calls from park. See Call Park, page 454. |
| 12.4(4)XC         | **Direct pickup of parked call on monitored park slot**—A call that is parked on a monitored call-park slot can be picked up by pressing the assigned monitor button. See Call Park, page 454. |
### Call Transfer

<table>
<thead>
<tr>
<th>Cisco IOS Release</th>
<th>Description</th>
</tr>
</thead>
</table>
| 12.4(4)XC        | **Call transfer blocking**—When call transfers to phones outside the Cisco Unified CME system have been globally enabled, you can block them for individualephones.  
See Call Transfer, page 465. |
| 12.4(4)XC        | **Call transfer destination digits limited**—When call transfers to phones outside the Cisco Unified CME system have been globally enabled, you can limit the number of digits that can be dialed when transferring a call for individual epophones.  
See Call Transfer, page 465 |
| 12.4(4)XC        | **transfer-system command**—The command default has been changed from the **blind** keyword to the **full-consult** keyword, making H.450.2 consultative transfer the default call transfer method.  
See Call Transfer, page 465 and Transfer and Forwarding Support, page 223. |

### Conference

<table>
<thead>
<tr>
<th>Cisco IOS Release</th>
<th>Description</th>
</tr>
</thead>
</table>
| 12.4(4)XC        | **Drop last party or keep parties connected**—New options for the **keep-conference** command can be configured per ephone to specify whether the last party that joined a conference can be dropped from the conference and whether the remaining two parties should be allowed to continue their connection after the conference initiator has left the conference.  
See Conferencing, page 480. |
| 12.4(4)XC        | **Improved conference display**—A Cisco Unified CME phone that is connected to a three-way conference displays “Conference.”  
No special configuration is required. |

### Ephone Hunt Groups

<table>
<thead>
<tr>
<th>Cisco IOS Release</th>
<th>Description</th>
</tr>
</thead>
</table>
| 12.4(4)XC        | **Maximum number of hunt groups** per Cisco Unified CME system has increased from 10 to 100.  
No special configuration is required. |
| 12.4(4)XC        | **Maximum number of agents** per hunt group has increased from 10 to 20.  
No special configuration is required. |
| 12.4(4)XC        | **Change in hops command default**—The maximum number of hops allowed by a hunt group is automatically adjusted to reflect the dynamically changing number of members.  
No special configuration is required. |
| 12.4(4)XC        | **Dynamic hunt group membership**—Agents can join or leave a preconfigured hunt group using standard or custom FACs when wildcard slots are configured for hunt groups and the agents’ ephone-dns are authorized to join hunt groups. An agent joining a hunt group uses a wildcard slot, and an agent leaving a group relinquishes the slot so that another agent can use it.  
See Ephone Hunt Groups, page 396. |
Table 14  Cisco Unified CME 4.0 Features  (Continued)

<table>
<thead>
<tr>
<th>Cisco IOS Release</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>12.4(4)XC</strong></td>
<td><strong>Agent status control</strong>—Hunt group agents can put their phones in a not-ready state to temporarily suspend the receiving of hunt group calls. The HLog soft key is provided to provide this functionality. It is a toggle: if an agent presses it while the phone is in a ready state, the phone is changed to a not-ready state. If the phone is in a not-ready state, it is changed to ready status. In this way, the HLog soft key allows agents to temporarily block hunt-group calls to their phones for short breaks without relinquishing their slots in the hunt group. A new FAC is also provided to toggle ready and not-ready status for an ephone-dn or for an ephone. See Ephone Hunt Groups, page 396.</td>
</tr>
<tr>
<td><strong>12.4(4)XC</strong></td>
<td><strong>Automatic agent not-ready status</strong>—The criterion for triggering a hunt group agent to be automatically placed into not-ready status (previously called automatic logout) has changed in this release. Previously, a hunt group agent was put into not-ready status (logged out) if he or she did not answer a hunt group call in less time than the time specified in the timeout command. In Cisco Unified CME 4.0 and later versions, if an agent does not answer the number of consecutive hunt-group calls that you specify in the auto logout command, the agent’s ephone-dn is put into not-ready status (logged out) and will not receive further hunt group calls. However, the agent still retains a hunt group slot. You can specify that an automatic change to not-ready status should be limited to dynamic hunt group members only, to static members only, or you can include both types of members. See Ephone Hunt Groups, page 396.</td>
</tr>
<tr>
<td><strong>12.4(4)XC</strong></td>
<td><strong>No-answer timeout enhancements</strong>—No-answer timeouts in ephone hunt groups can be set individually for each ephone-dn in the list. A maximum cumulative no-answer timeout can be also be set. See Ephone Hunt Groups, page 396.</td>
</tr>
<tr>
<td><strong>12.4(4)XC</strong></td>
<td><strong>Longest-idle hunt group improvement</strong>—The algorithm of choosing the next agent to receive a call in a longest-idle hunt group is based on on-hook time stamps. The agent with the smallest on-hook time stamp value will be chosen when the next call comes to the hunt group. The default behavior is that an on-hook time stamp value is updated only when an agent answers a call. A new command, the from-ring command, specifies that on-hook time stamps should be updated when a call rings an agent as well as when a call is answered by an agent. On-hook time stamps can be displayed using the show ephone-hunt command. See Ephone Hunt Groups, page 396.</td>
</tr>
<tr>
<td><strong>12.4(4)XC</strong></td>
<td><strong>Restricting presentation of calls to idle or on-hook phones</strong>—The presentation of ephone hunt group calls can be restricted to hunt-group members on phones that are idle or phones that are on-hook. Normally, a hunt group call is presented to a phone when the ephone-dn that is a member of the hunt group is free, regardless of the state of the other ephone-dns on the phone. This enhancement considers all lines on the phone, both members of the hunt group and non-members, when restricting presentation of hunt group calls. See Ephone Hunt Groups, page 396.</td>
</tr>
<tr>
<td><strong>12.4(4)XC</strong></td>
<td><strong>Return to transferring party on no answer in an ephone hunt group</strong>—A call that was transferred into a hunt group and that cycles through the hunt group without being answered can be returned to the party that transferred it to the hunt group instead of being sent to voice mail or another final destination. See Ephone Hunt Groups, page 396.</td>
</tr>
</tbody>
</table>
### Table 14  Cisco Unified CME 4.0 Features  (Continued)

<table>
<thead>
<tr>
<th>Cisco IOS Release</th>
<th>Description</th>
</tr>
</thead>
</table>
| 12.4(4)XC         | **Return to a secondary destination in an ephone hunt group after call park**—Calls that are parked by hunt group agents can be returned to a different entry point in the hunt group.  
See Ephone Hunt Groups, page 396. |
| 12.4(4)XC         | **Local call forwarding restriction in sequential ephone hunt groups**—In sequential ephone-hunt groups only, local (internal) calls to the hunt group can be prevented from being forwarded beyond the first ephone-dn in the hunt group, even when that ephone-dn does not answer or is busy.  
See Ephone Hunt Groups, page 396. |
| 12.4(4)XC         | **Enhanced display of ephone hunt-group information**—A configurable text string can be added to provide information in configuration output and to be displayed on IP phones when a hunt-group call is ringing or answered. This text string can be used to indicate the name or purpose of the hunt group.  
A configurable text string can be added to be displayed on IP phones when all hunt-group members are logged out. This text string can be used to indicate where calls are being sent at that time; for example, to night service or voice mail.  
See Ephone Hunt Groups, page 396. |

### Ephone Templates and Ephone-dn Templates

<table>
<thead>
<tr>
<th>Cisco IOS Release</th>
<th>Description</th>
</tr>
</thead>
</table>
| 12.4(4)XC         | **Maximum number of ephone templates** that can be defined has increased from 5 to 20.  
No special configuration is required. |
| 12.4(4)XC         | **New commands available for ephone templates**—Ephone templates were previously introduced to allow system administrators to control the display of soft keys in various call states on individual ephones. Their role has been expanded to allow you to define a set of ephone parameter values that can be assigned to one or more phones in a single step.  
See Ephone Templates, page 318. |
| 12.4(4)XC         | **Ephone-dn templates** are introduced to allow administrators to easily apply sets of configured parameters to individual ephone-dns. Up to 15 ephone-dn templates can be defined.  
See Ephone-dn Templates, page 322. |

### Phone Features

<table>
<thead>
<tr>
<th>Cisco IOS Release</th>
<th>Description</th>
</tr>
</thead>
</table>
| 12.4(4)XC         | **Overlaid ephone-dns**—The maximum number of overlaid ephone-dns per ephone button has increased from 10 to 25.  
No special configuration is required. |
| 12.4(4)XC         | **Overlaid ephone-dn call-waiting display**—The number of waiting calls that can be displayed for overlaid ephone-dns that have call waiting configured has been increased to six for the following phone types: Cisco IP Phone 7940G, 7941G, 7941G-GE, 7960G, 7961G, 7961G-GE, 7970G, and 7971G-GE.  
The overlaid ephone-dns must be configured on the phone using the **button** command and the **c** keyword.  
See Overlaid Ephone-dns, page 429. |
Cisco Unified CME 4.0

Table 14  Cisco Unified CME 4.0 Features  (Continued)

<table>
<thead>
<tr>
<th>Cisco IOS Release</th>
<th>Description</th>
</tr>
</thead>
</table>
| 12.4(4)XC | **Overlaid ephone-dn call overflow to other buttons**—One or more buttons can be dedicated to serve as expansion, or overflow, buttons for another button on the same Cisco Unified IP phone that has overlaid ephone-dns. A call to an overlay button that is busy with an active call will roll over to the next available expansion button.  
  See Overlaid Ephone-dns, page 429. |
| 12.4(4)XC | **Headset auto-answer**—When the headset key on a phone is activated, lines on the phone that are specified for headset auto-answer will automatically connect to incoming calls after playing an alerting tone to notify the phone user of the incoming call. This feature is available only on Cisco Unified IP phones 7940G, 7960G, 7970G, and 7971G-GE.  
  See Headset Auto-Answer, page 508. |
| 12.4(4)XC | **Distinctive ringing**—An extension’s ring patterns can be set to distinguish among internal, external, and feature calls.  
  See Distinctive Ringing, page 502. |
| 12.4(4)XC | **Soft-key control for hold state**—Ephone templates have been enhanced to allow modification of the soft keys that are available to a phone while a call is on hold. The NewCall and Resume soft keys are normally available when a phone has a call on hold, but a template can be applied to the phone to remove the NewCall soft key, for example.  
  See Soft-Key Display, page 551. |
| 12.4(4)XC | **Line-selectable MWI**—Previously, the message-waiting indication (MWI) lamp on a phone could only indicate when messages were waiting for the primary number on a phone. Now any phone line can be designated during configuration.  
  See MWI Line Selection, page 519. |
| 12.4(4)XC | **PC port disable**—System administrators can disable PC ports globally in the telephony-service configuration or individually in the phone configuration by using an ephone template.  
  See PC Port Disable, page 564 |

Phone Support

<table>
<thead>
<tr>
<th>Cisco IOS Release</th>
<th>Description</th>
</tr>
</thead>
</table>
| 12.4(4)XC | **Cisco IP Communicator** is a software-based application that delivers enhanced telephony support on personal computers. This SCCP-based application allows computers to function as IP phones, providing high-quality voice calls on the road, in the office, or from wherever users may have access to the corporate network. Cisco IP Communicator appears on a user’s computer monitor as a graphical, display-based IP phone with a color screen, a key pad, feature buttons, and soft keys. Cisco Unified CME 4.0 supports Cisco IP Communicator 2.0 and later versions.  
  See Cisco IP Communicator, page 140 |
| 12.4(4)XC | **Teleworker remote phone**—Teleworkers can connect remote phones over a WAN and be directly supported by a Cisco Unified CME system.  
  See Teleworker Remote Phones, page 143 |
### Feature History

**Cisco Unified CME 4.0**

12.4(4)XC

**New IP phone support**
- Cisco Unified IP Phone 7911G
- Cisco Unified IP Phone 7941G and Cisco Unified IP Phone 7941G-GE
- Cisco Unified IP Phone 7961G and Cisco Unified IP Phone 7961G-GE

No additional configuration is required for these phones. They are supported in the appropriate Cisco IOS commands.

### Security Features

12.4(4)XC

**Cisco Unified CME phone authentication** is a security infrastructure for providing secure Skinny Client Control Protocol (SCCP) signaling between Cisco Unified CME and IP phones.

See [Phone Authentication](#), page 149.

### User Features

12.4(4)XC

**Feature Access Code (FAC) support**—The same FACs that are used by analog phones can be enabled for IP phones. In addition, standard FACs can be customized and aliases can be created to simplify the dialing of a FAC and any additional digits that are required to activate the feature.

See [Feature Access Codes](#), page 325.

12.4(4)XC

**Feature control**—The following soft key features can be individually blocked per ephone: CFwdAll, Confrn, GpickUp, Park, PickUp, and Trnsfer.

See [Feature Control](#), page 329.

12.4(4)XC

**Directed call pickup disable**—The `no service directed-pickup` command globally disables directed call pickup and changes the action of the PickUp soft key on IP phones to invoke local group pickup rather than directed call pickup.

See [Call Pickup](#), page 385.

12.4(4)XC

**Blocking call forwarding of local calls**—The call-forwarding feature for ephone-dns can be set to prevent the forwarding of local (internal) calls from other Cisco Unified CME ephones. External calls will continue to be forwarded as specified by the configuration for the ephone-dns.

See [Call Forwarding](#), page 372.

12.4(4)XC

**Call waiting displays for overlay ephone-dns**—The maximum number of call-waiting calls that can be presented to an overlay ephone-dns with call waiting has been increased to six. This maximum is not supported on Cisco IP Phones 7905, 7911, and 7912, which support the display of a maximum of two call-waiting calls.

No special configuration is required.
### Feature History

#### Video Support

<table>
<thead>
<tr>
<th>Cisco IOS Release</th>
<th>Description</th>
</tr>
</thead>
</table>
| 12.4(4)XC         | **Video support for SCCP-based endpoints**—This feature adds video support for the Cisco Unified CallManager Express to maintain close feature parity with Cisco Unified CallManager. This feature allows you to pass a video stream with a voice call, between video-capable SCCP endpoints and between SCCP and H.323 endpoints. Through the Cisco Unified CME router, the video-capable endpoints can communicate with each other locally, to a remote H.323 endpoint through a gateway, or through an H.323 network.  
See Video Support for SCCP-Based Endpoints, page 285. |

#### Administrative Features

<table>
<thead>
<tr>
<th>Cisco IOS Release</th>
<th>Description</th>
</tr>
</thead>
</table>
| 12.4(4)XC         | **VLAN CoS marking**—In Cisco Unified CME 4.0 and later releases, there is a change in the way that packets are sent to IP phones. Cisco CME will no longer automatically process Layer-3-to-Layer-2 VLAN Class of Service (CoS) priority marking. If you need to configure L3-to-L2 marking, you can do so on the Cisco Unified CME router, as explained in the Enterprise QoS Solution Reference Network Design Guide.  
Cisco Unified CME will continue to mark Layer 3, but Layer 2 marking is now only handled in the Cisco IOS software. If your Quality of Service (QoS) design requires Layer 2 marking, it will have to be explicitly configured, either on a Catalyst switch that supports this capability or on the Cisco Unified CME router under the Ethernet interface configuration.  
This change affects customers who use IEEE 802.1Q (Dot1q) or InterSwitch Link (ISL) configurations on the Ethernet interfaces between their Cisco Unified CME router and the Ethernet switch that connects to their IP phones.  
For more information, see the Enterprise QoS Solution Reference Network Design Guide. |
| 12.4(4)XC         | **QSIG supplementary services support**—H.450 supplementary services features allow Cisco Unified CME phones to use QSIG to interwork with PBX phones in a seamless fashion. IP phones can use a PBX message center with proper MWI notifications.  
See QSIG Supplementary Services, page 270. |
| 12.4(4)XC         | **Fax passthrough mode** is now supported using Cisco VG 224 voice gateways, Analog Telephone Adaptors (ATA), and SCCP.  
ATAs ship with SIP firmware, so SCCP firmware must be loaded before this feature can be used. For information about loading phone firmware files, see Upgrading Individual Phone Firmware Files, page 50. |
| 12.4(4)XC         | **External storage of configuration files and per-phone configuration files**—Phone configuration files can be stored on an external TFTP server to offload the TFTP server function of the Cisco Unified CME router. The use of this additional storage space permits the use of per-phone configuration files, which can be used to specify different user locales and network locales for phones in a single Cisco Unified CME system.  
See Externally Stored and Per-Phone Configuration Files, page 93. |
| 12.4(4)XC         | **Alternative user locales and network locales**—Up to five user-locale codes and network-locale codes can be used in a single Cisco Unified CME system, by identifying them as alternative codes. The alternative codes then are made part of ephone templates, which can be applied to individual ephones.  
See Alternative User and Network Locales, page 97. |
<table>
<thead>
<tr>
<th>Cisco IOS Release</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4(4)XC</td>
<td><strong>User-defined user locales and network locales</strong>—You can define up to five user locales and network locales that can be used for any phone in the Cisco Unified CME system. The user-defined codes can then be applied to ephones as alternative or default codes. See User-Defined User and Network Locales, page 105.</td>
</tr>
<tr>
<td>12.4(4)XC</td>
<td><strong>Music on hold (MOH) for internal calls</strong>—In Cisco Unified CME 4.0 and later releases, internal callers (those making calls between extensions in the same Cisco Unified CME system) hear music when they are on hold or are being transferred. There are no new commands, but the <code>multicast moh</code> command must be used to enable the flow of packets to the subnet on which the phones are located. Internal extensions that are connected through an analog voice gateway (Cisco VG 224) or through a WAN (remote extensions) do not hear MOH on internal calls. A remote extension may hear MOH if the phone is not set up to use a media termination point and the multicast network is set up correctly. The ability to disable multicast MOH per phone was introduced, using the <code>no multicast-moh</code> command in ephone or ephone-template configuration mode. See Music on Hold, page 333.</td>
</tr>
<tr>
<td>12.4(4)XC</td>
<td><strong>Night service</strong> configuration is simplified with the addition of keywords <em>everyday</em>, <em>weekend</em>, and <em>weekday</em>. See Night Service, page 420.</td>
</tr>
<tr>
<td>12.4(4)XC</td>
<td><strong>Phone substitution without loss of configuration information</strong>—A MAC address can be replaced in a phone configuration to indicate that a physical instrument has been replaced without the loss of the phone’s configuration information. No special configuration is required for this feature.</td>
</tr>
<tr>
<td>12.4(4)XC</td>
<td><strong>Disabling gatekeeper registration</strong>—Registration to an H.323 gatekeeper or SIP proxy can be disabled globally using the <code>max-dn</code> command. The default is that registration is enabled. Registration can be disabled on a per-phone basis using the <code>number</code> command when global registration is enabled. See Task 5: Setting Cisco Unified CME Parameters, page 60.</td>
</tr>
<tr>
<td>12.4(4)XC</td>
<td><strong>Disabling automatic phone registration</strong>—Normally, Cisco Unified CME allocates an ephone slot to any ephone that connects to the system. To prevent unauthorized registrations, the <code>no auto-reg-ephone</code> command prevents any ephone from registering with Cisco Unified CME if its MAC address is not explicitly listed in the configuration. See Task 5: Setting Cisco Unified CME Parameters, page 60.</td>
</tr>
<tr>
<td>12.4(4)XC</td>
<td><strong>Prefix option for SIP unsolicited MWI Notify messages</strong>—Central voice-message servers that provide mailboxes for multiple Cisco Unified CME sites may use site codes or prefixes to distinguish among similarly numbered ranges of extensions at different sites. Unsolicited message-waiting indication (MWI) Notify messages from Session Interface Protocol (SIP) voice-message servers are sent to Cisco Unified CME in order to light MWI lamps on phones. An MWI Notify message can contain a site prefix in addition to the extension number of the phone that has a message. A new keyword for the <code>mwi sip-server</code> command allows you to specify the prefix for your site so that central mailbox numbers are correctly converted to your extension numbers. See MWI Prefix Specification for SIP Voice-Mail Applications, page 308.</td>
</tr>
<tr>
<td>Cisco IOS Release</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>12.4(4)XC</td>
<td><strong>Mailbox selection policy for voice-mail servers</strong>—A policy can be set for selecting the mailbox to use for calls that are diverted one or more times within a Cisco Unified CME system before being sent to a Cisco Unity Express, Cisco Unity, or PBX voice-mail pilot number. See <a href="#">Mailbox Selection Policy for Voice-Mail Servers, page 304</a>.</td>
</tr>
<tr>
<td>12.4(4)XC</td>
<td><strong>Bulk-loading of speed-dial numbers</strong>—Text files containing lists of speed-dial numbers can be loaded into system flash or at a URL. The files can hold up to 10,000 numbers and can be applied to all phones or to specified phones. See <a href="#">Speed Dial, page 523</a>.</td>
</tr>
<tr>
<td>12.4(4)XC</td>
<td><strong>Failover to Redundant Router</strong>—Sites can be set up with a primary and secondary Cisco Unified CME router to provide redundant Cisco Unified CME capability. Phones automatically register at the secondary router if the primary router fails and later rehome to the primary router when it is operational again. See <a href="#">Redundant Router, page 351</a>.</td>
</tr>
<tr>
<td>12.4(4)XC</td>
<td><strong>SCCP state debugging</strong>—To assist with troubleshooting, the <code>debug ephone sccp-state</code> command is introduced. This command outputs only the debug messages that correspond to the SCCP messages that are sent to IP phones to indicate the SCCP phone call state. See the <a href="#">Cisco Unified CallManager Express (All Versions) Command Reference</a>.</td>
</tr>
<tr>
<td>12.4(4)XC</td>
<td><strong>TAPI enhancements</strong>—The Telephony Application Programming Interface (TAPI) service provider (TSP) API acts as an interface between TAPI and Cisco Unified CME to allow TAPI-based applications to provide call control to the IP phones on the Cisco Unified CME system. An updated version of the TSP interface is provided with this release to increase the functionality of TAPI-based applications with Cisco Unified CME calls. See the link to the TAPI documentation at the <a href="#">Cisco Unified CME Documentation Roadmap</a>.</td>
</tr>
<tr>
<td>12.4(4)XC</td>
<td><strong>XML interface enhancements</strong>—An eXtensible Markup Language (XML) application program interface (API) is provided to supply data from Cisco Unified CME to management software. In Cisco Unified CME 4.0 and later versions, the XML interface is provided through the IOS XML Infrastructure (IXI), in which the parser and transport layers are separated from the application itself. This modularity provides scalability and enables future XML supports to be developed. In Cisco Unified CME 4.0 and later versions, all Cisco Unified CME features have XML support. See <a href="#">XML Application Programming Interface, page 360</a>.</td>
</tr>
</tbody>
</table>
Cisco Unified CallManager Express Overview

Cisco Unified CallManager Express (Cisco Unified CME) is a call-processing application in Cisco IOS software that enables Cisco routers to deliver key-system or hybrid PBX functionality for enterprise branch offices or small businesses. This chapter contains the following sections:

- Cisco Unified CallManager Express Overview, page 21
- Basic Cisco Unified CME Concepts, page 24
- Additional References, page 35

Note
Prior to version 4.0, the name of this product was Cisco CallManager Express (Cisco CME). Prior to version 3.0, the name was Cisco IOS Telephony Services (Cisco ITS).

Note

Cisco Unified CallManager Express Overview

Cisco Unified CallManager Express is a feature-rich entry-level IP telephony solution that is integrated directly into Cisco IOS software. Cisco Unified CallManager Express allows small business customers and autonomous small enterprise branch offices to deploy voice, data, and IP telephony on a single platform for small offices, thereby streamlining operations and lowering network costs.

Cisco Unified CME is ideal for customers who have data connectivity requirements and also have a need for a telephony solution in the same office. Whether offered through a service provider’s managed services offering or purchased directly by a corporation, Cisco Unified CME offers most of the core telephony features required in the small office, as well as many advanced features not available with traditional telephony solutions. Being able to deliver IP telephony and data routing using a single converged solution allows customers to optimize their operations and maintenance costs, resulting in a very cost-effective solution that meets office needs.
Cisco Unified CallManager Express Network Scenarios

Figure 1 shows a typical deployment of a Cisco Unified CallManager Express (Cisco Unified CME) router with several Cisco IP phones connected to it. The Cisco Unified CME router is connected to the PSTN. The router can also connect to a gatekeeper and a RADIUS billing server in the same network.

Figure 2 shows a branch office with several Cisco Unified IP phones connected to a Cisco IAD2430 series router using Cisco Unified CME. The Cisco IAD2430 router is connected to a multiservice router at a service provider office. The multiservice router at the service provider office provides connection to the WAN and PSTN.
Additional Features

Provisioning

The router provides a mechanism to provision Cisco Unified CallManager Express, which allows you to perform the following functions:

- Assign extension numbers to the line appearances on each Cisco Unified IP phone.
- Assign numbers to the speed-dial buttons on each Cisco Unified IP phone.
- Assign caller identification information to each extension number.
- Assign extension numbers to phones other than Cisco Unified IP phones attached to the system by using the standard voice-port and dial-peer configuration command-line interface (CLI).
- Provide dial-plan information to route calls to either PSTN lines or voice network connections.

For installation information, see the “Installing Cisco Unified CME” section on page 43.

Connecting Cisco IP Phones

Cisco Unified IP phones can be connected to and disconnected from the Cisco Unified CallManager Express router without requiring a router reboot or manual status reset, a process sometimes called “hot-plugging.”
Basic Cisco Unified CME Concepts

The following sections explain concepts that will help you to design and configure Cisco Unified CME systems.

- System Design, page 24
- Ephones, page 25
- Ephone-dns, page 25
- Phone Number Plan, page 32
- Direct Inward Dialing, page 33
- PBX or Keyswitch Model, page 33

System Design

Cisco Unified CME systems are extremely flexible because they are modular. A Cisco Unified CME system consists of a router that serves as a gateway and one or more VLANs that connect IP phones and phone devices to the router. In addition, a Cisco Unified CME system uses the following basic building blocks:

- **Ephone**—A software construct that usually represents a physical telephone instrument, although it is also used to represent a port that connects to a voice-mail system. The ephone construct provides the ability to configure the physical instrument using Cisco IOS software. Each ephone can have multiple extensions associated with it in a many-to-many relationship, and a single extension can be associated with multiple ephones so that it appears as a shared extension. The maximum number of ephones in a Cisco Unified CME system is the maximum number of physical instruments that can be connected to the system.

- **Ephone-dn**—A software construct that represents the line that connects a voice channel to a phone instrument on which a user can receive and make calls. An ephone-dn represents a virtual voice port in the Cisco Unified CME system, so the maximum number of ephone-dns in a Cisco Unified CME system is the maximum number of simultaneous call connections that can occur. Note that this concept is different from the maximum number of physical lines in a traditional telephony system and also is different from the maximum number of telephone or extension numbers that can be assigned.

Traditional telephony systems are based on physical connections and are therefore limited in the types of phone service that they can offer. Because the ephone and ephone-dn are software constructs and because the audio stream is packet-based, an almost limitless number of combinations of phone numbers, lines, and phones can be planned and implemented.

Cisco Unified CME systems can be designed in many ways. The key is to determine how many simultaneous calls you want to be able to handle at your site and at each phone at your site, how many different numbers you want to have, and how many phones you want to have. Even a Cisco Unified CME system has its limits, however. The following factors should be considered in your system design:

- Maximum number of ephones—There is a maximum number of ephones per system. This number corresponds to the maximum number of devices that can be attached. The maximum is platform- and version-dependent. To find the maximum for your platform and version, see the *Cisco Unified CallManager Express Supported Firmware, Platforms, Memory, and Voice Products* document that is listed under your Cisco Unified CME version.
• Maximum number of ephone-dns—There is a maximum number of ephone-dns per system. This number corresponds to the maximum number of simultaneous call connections that can occur. The maximum is platform- and version-dependent. To find the maximum for your platform and version, see the Cisco Unified CallManager Express Supported Firmware, Platforms, Memory, and Voice Products document that is listed under your Cisco Unified CME version.

• Maximum number of telephone numbers—Your numbering plan may restrict the range of telephone numbers or extension numbers that you can use. For example, if you have DID, the PSTN may assign you a certain series of numbers.

• Maximum number of buttons per phone—You may be limited by the number of buttons and phones that your site can use. For example, you may have two people with six-button phones to answer twenty different telephone numbers.

The flexibility of a Cisco Unified CME system is due largely to the different types of ephone-dns that you can assign to phones in your system. By understanding the types of ephone-dns and considering how they can be combined, you can create the complete call coverage that your business requires. For more information about types of ephone-dns, see the “Ephone-dns” section on page 25.

After setting up the ephone-dns and ephones that you need, you add optional Cisco Unified CME features to create a telephony environment that enhances your business objectives. Cisco Unified CME systems are able to integrate with the PSTN and with your business requirements to allow you to continue using your existing number plans, dialing schemes, and call coverage patterns.

Ephones

An ephone, or “Ethernet phone,” is a single instance of the software configuration of the physical instrument with which a phone user makes and receives calls in a Cisco Unified CME system. The physical ephone is either a Cisco Unified IP phone or an analog phone equipped with an analog telephone adaptor (ATA) device.

Each ephone has a unique phone-tag, or sequence number, to identify it during configuration. The maximum number of ephones per system is platform- and version-dependent and is listed in the Cisco Unified CallManager Express Supported Firmware, Platforms, Memory, and Voice Products document for your Cisco Unified CME version.

An ephone is populated with ephone-dns and features by the ephone command, which associates the MAC address of a physical phone with the telephone numbers associated with ephone-dns and with other Cisco Unified CME features.

Ephone-dns

An ephone-dn, or “Ethernet phone directory number,” is a software construct that represents the line that connects a voice channel to a phone instrument on which a user can receive and make calls. An ephone-dn has one or more extension or telephone numbers associated with it to allow call connections to be made. An ephone-dn is equivalent to a phone line in most cases, but not always. There are several types of ephone-dns, which have different characteristics. The maximum number of ephone-dns per system is platform- and version-dependent and is listed in the Cisco Unified CallManager Express Supported Firmware, Platforms, Memory, and Voice Products document for your Cisco Unified CME version.

Each ephone-dn has a unique dn-tag, or sequence number, to identify it during configuration. Ephone-dns are assigned to line buttons on ephones during configuration.
An ephone-dn is created by the `ephone-dn` command, which automatically builds one virtual voice port and one or more dial peers for the ephone-dn, depending on your dial-plan pattern and whether there is an entry in the secondary number field of the `ephone-dn` command. The `ephone-dn` command automates the process of associating dial peers to an ephone-dn’s virtual voice port and manages the numbering and configuring of virtual voice ports. Dial peers that are created by the `ephone-dn` command can be reviewed using the `show telephony-service dial-peer` command. They are not displayed by the `show running-config` command.

The number of ephone-dns that you create corresponds to the number of simultaneous calls that you can have, because each ephone-dn represents a virtual voice port in the router. This means that if you want more than one call to the same number to be answered simultaneously, you need multiple virtual voice ports (ephone-dns) with the same destination pattern (extension or telephone number).

The ephone-dn is the basic building block of a Cisco Unified CME system. Six different types of ephone-dn can be combined in different ways for different call coverage situations. Each type will help with a particular type of limitation or call-coverage need. For example, if you want to keep the number of ephone-dns low and provide service to a large number of people, you might use shared ephone-dns. Or if you have a limited quantity of extension numbers that you can use but you need to have a large quantity of simultaneous calls, you might create two or more ephone-dns with the same number. The key is knowing how each type of ephone-dn works and what its advantages are.

The following sections will help you understand the types of ephone-dn in a Cisco Unified CME system:

- Single-Line Ephone-dn
- Dual-Line Ephone-dn
- Two Ephone-dns with One Number
- Dual-Number Ephone-dn
- Shared Ephone-dn
- Overlaid Ephone-dn

### Single-Line Ephone-dn

A single-line ephone-dn has the following characteristics:

- Makes one call connection at a time using one phone line button. A single-line ephone-dn has one telephone number associated with it.

- Should be used when phone buttons have a one-to-one correspondence to the PSTN lines that come into a Cisco Unified CME system.

- Should be used for lines that are dedicated to intercom, paging, message-waiting indicator (MWI), loopback, and music-on-hold (MOH) feed sources.

- When used with multiple-line features like call waiting, call transfer, and conferencing, there must be more than one single-line ephone-dn on a phone.

- Can be combined with dual-line ephone-dns on the same phone.

Note that you must make the choice to configure each ephone-dn in your system as either dual-line or single-line when you initially create ephone-dn configuration entries. If you need to change from single-line to dual-line later, you must delete the ephone-dn and then recreate it.

Figure 3 shows a single-line ephone-dn.
Dual-Line Ephone-dn

A dual-line ephone-dn has the following characteristics:

- Can make two call connections at the same time using one phone line button. A dual-line ephone-dn has two channels for separate call connections.
- Can have one number or two numbers (primary and secondary) associated with it.
- Should be used for an ephone-dn that needs to use one line button for features like call waiting, call transfer, or conferencing.
- Cannot be used for lines that are dedicated to intercom, paging, message-waiting indicator (MWI), loopback, and music-on-hold (MOH) feed sources.
- Can be combined with single-line ephone-dns on the same phone.

Note that you must make the choice to configure each ephone-dn in your system as either dual-line or single-line when you initially create ephone-dn configuration entries. If you need to change from single-line to dual-line later, you must delete the ephone-dn and then recreate it.

Figure 4 shows a dual-line ephone-dn.

Two Ephone-dns with One Number

Two ephone-dns with one number have the following characteristics:

- Have the same telephone number but two separate virtual voice ports, and therefore can have two separate call connections.
- Can be single-line or dual-line ephone-dns.
- Can appear on the same phone on different buttons or on different phones.
- Should be used when you want the ability to make more call connections while using fewer numbers.

Figure 5 on page 28 shows a phone with two buttons that have the same number, extension 1003. Each button has a different ephone-dn (button 1 is ephone-dn 13 and button 2 is ephone-dn 14), so each button can make one independent call connection if the ephone-dns are single-line and two call connections (for a total of four) if the ephone-dns are dual-line.
Figure 6 shows two phones that each have a button with the same number. Because the buttons have different ephone-dns, the calls that are connected on these buttons are independent of one another. The phone user at phone 4 can make a call on extension 1003, and the phone user on phone 5 can receive a different call on extension 1003 at the same time.

The two ephone-dns-with-one-number situation is different than a shared line, which also has two buttons with one number but has only one ephone-dn for both of them. A shared ephone-dn will have the same call connection at all the buttons on which the shared ephone-dn appears. If a call on a shared ephone-dn is answered on one phone and then placed on hold, the call can be retrieved from the second phone on which the shared ephone-dn appears. But when there are two ephone-dns with one number, a call connection appears only on the phone and button at which the call is made or received. In the example in Figure 6, if the user at phone 4 makes a call on button 1 and puts it on hold, the call can be retrieved only from phone 4. For more information about shared lines, see the “Shared Ephone-dn” section on page 29.

The examples in Figure 5 and Figure 6 show how two ephone-dns with one number are used to provide a small hunt group capability. In Figure 5, if the ephone-dn on button 1 is busy or does not answer, an incoming call to extension 1003 rolls over to the ephone-dn associated with button 2 because the preference and no huntstop commands have been used. Similarly, if button 1 on phone 4 is busy, an incoming call to 1003 rolls over to button 1 on phone 5. Values assigned in the preference command are passed to the dial peers created by the two ephone-dns. Both dial peers for the ephone-dns are matched when this extension number is dialed, and the call is connected to the ephone-dn with the highest preference. The default preference value is 0 (the highest value), so ephone-dn 13 on button 1 gets the first call. The no huntstop command tells the dial peers not to stop hunting for another match, so the second call to extension 1003 is sent to ephone-dn 14.

Figure 5 Two Ephone-dns with One Number on One Phone

Figure 6 Two Ephone-dns with One Number on Two Phones
Dual-Number Ephone-dn

A dual-number ephone-dn has the following characteristics:

- Has two telephone numbers, a primary number and a secondary number.
- Can make one call connection if it is a single-line ephone-dn.
- Can make two call connections at a time if it is a dual-line ephone-dn.
- Should be used when you want to have two different numbers for the same button without using more than one ephone-dn.

Figure 7 shows an ephone-dn that has two numbers, extension 1006 and extension 1007.

Figure 7  Dual-Number Ephone-dn

Shared Ephone-dn

A shared ephone-dn has the following characteristics:

- Appears on two different phones but uses the same ephone-dn and number.
- Can make one call at a time and that call appears on both phones.
- Should be used when you want the capability to answer or pick up a call at more than one phone.

Because these phones share the same ephone-dn, if the ephone-dn is connected to a call on one phone, that ephone-dn is unavailable for other calls on the second phone. If a call is placed on hold on one phone, it can be retrieved on the second phone. This is like having a single-line phone in your house with multiple extensions. You can answer the call from any phone on which the number appears, and you can pick it up from hold on any phone on which the number appears.

Figure 8 shows a shared ephone-dn. Extension 1008 appears on both phone 7 and phone 8.

Figure 8  Shared Ephone-dn
Overlaid Ephone-dn

An overlaid ephone-dn has the following characteristics:

- Is a member of an overlay set, which includes all the ephone-dns that have been assigned together to a particular phone button.
- Can have the same telephone or extension number as other members of the overlay set or different numbers.
- Can be single-line or dual-line, but cannot be mixed single-line and dual-line in the same overlay set.
- Can be shared on more than one phone.

Overlaid ephone-dns provide call coverage similar to shared ephone-dns because the same number can appear on more than one phone. The advantage of using two ephone-dns in an overlay arrangement rather than as simple shared ephone-dns is that a call to the number on one phone does not block the use of the same number on the other phone, as would happen if this were a shared ephone-dn.

You can overlay up to 25 lines on a single button. A typical use of overlaid ephone-dns would be to create a “10x10” shared line, with ten lines in an overlay set shared by ten phones, resulting in the possibility of ten simultaneous calls to the same number.

Figure 9 on page 30 shows an overlay set with two ephone-dns and one number that is shared on two phones. Ephone-dn 17 has a default preference value of 0, so it will receive the first call to extension 1001. The phone user at phone 9 answers the call, and a second incoming call to extension 1001 can be answered on phone 10 using ephone-dn 18.

A more complex ephone-dn configuration mixes overlaid ephone-dns with shared ephone-dns and plain dual-line ephone-dns on the same phones. Figure 10 on page 31 illustrates the following example of a manager with two assistants. On the manager’s phone the same number, 2001, appears on button 1 and button 2. The two line appearances of extension 2001 use two single-line ephone-dns, so the manager can have two active calls on this number simultaneously, one on each button. The ephone-dns are set up so that button 1 will ring first, and if a second call comes in, button 2 will ring. Each assistant has a personal ephone-dn and also shares the manager’s ephone-dns. Assistant 1 has all three ephone-dns in an overlay set on one button, whereas assistant 2 has one button for the private line and a second button with both of the manager’s lines in an overlay set. A sequence of calls might be as follows.

1. An incoming call is answered by the manager on extension 2001 on button 1 (ephone-dn 20).
2. A second call rings on 2001 and rolls over to the second button on the manager’s phone (ephone-dn 21). It also rings on both assistants’ phones, where it is also ephone-dn 21, a shared ephone-dn.
3. Assistant 2 answers the call. This is a shared overlay line (one ephone-dn, 21, is shared among three phones, and on two of them this ephone-dn is part of an overlay set). Because it is shared with button 2 on the manager’s phone, the manager can see when assistant 2 answers the call.

4. Assistant 1 makes an outgoing call on ephone-dn 22. The button is available because of the additional ephone-dns in the overlay set on the assistant 1 phone.

At this point, the manager is in conversation on ephone-dn 20, assistant 1 is in conversation on ephone-dn 22, and assistant 2 is in conversation on ephone-dn 21.

**Note**

For more information and configuration steps, see the “Overlaid Ephone-dns” section on page 429.

**Figure 10**  Overlaid Ephone-dn (Complex Case)

- Manager phone
  - Button 1 is extension 2001
  - Button 2 is extension 2001

- Assistant 1 phone
  - Button 1 is extension 2001
  - Button 2 is extension 2002

- Assistant 2 phone
  - Button 1 is extension 2003
  - Button 2 is extension 2001

- ephone-dn 20
  - number 2001
  - no huntstop
  - ! Manager number

- ephone-dn 21
  - number 2001
  - preference 1
  - ! Manager number

- ephone-dn 22
  - number 2002
  - ! Assistant 1 personal number

- ephone-dn 23
  - number 2003
  - ! Assistant 2 personal number

- ephone 8
  - button 1:20 2:21
  - ! Manager phone

- ephone 9
  - button 1o22,20,21
  - ! Assistant 1 phone

- ephone 10
  - button 1:23 2o20,21
  - ! Assistant 2 phone
Phone Number Plan

If you are installing a Cisco Unified CME system to replace an older telephony system that had an established telephone number plan, you can retain the old number plan. Cisco Unified CME supports flexible extension number lengths and can provide automatic conversion between extension dialing and E.164 public telephone number dialing.

A successful Cisco Unified CME system requires a telephone numbering plan that supports future expansion. The numbering plan also must not overlap or conflict with other numbers that are on the same VoIP network or are part of a centralized voice mail system.

Cisco Unified CME supports shared lines as well as multiple lines configured with the same extension number. This means that you can set up several phones to share an extension number to provide coverage for that number. You can also assign several line buttons on a single phone to the same extension number to create a small hunt group. For more information about types of line configurations, see the “Ephone-dns” section on page 25.

If you are configuring more than one Cisco Unified CME site, you need to decide how calls between the sites will be handled. Calls between Cisco Unified CME phones can be routed either through the PSTN or over VoIP. If you are routing calls over VoIP, you must decide among the following three choices:

- You can route calls using a global pool of fixed-length extension numbers. For example, all sites have unique extension numbers in the range 5000 to 5999, and routing is managed by a gatekeeper. If you select this method, you should assign a subrange of extension numbers to each site so that duplicate number assignment does not result. You will have to keep careful records of which Cisco Unified CME system is assigned which number range.

- You can route calls using a local extension number plus a special prefix for each Cisco Unified CME site. This choice allows you to use the same extension numbers at more than one site.

- You can use an E.164 PSTN phone number to route calls over VoIP between Cisco Unified CME sites. In this case, intersite callers use the PSTN area code and local prefix to route calls between Cisco Unified CME systems.

If you choose to have a gatekeeper route calls among multiple Cisco Unified CME systems, you may face additional restrictions on the extension number formats that you use. For example, you might be able to register only PSTN-formatted numbers with the gatekeeper. The gatekeeper might not allow the registration of duplicate telephone numbers in different Cisco Unified CME systems, but you might be able to overcome this limitation. Cisco Unified CME allows the selective registration of either 2- to 5-digit extension numbers or 7- to 10-digit PSTN numbers, so registering only PSTN numbers might prevent the gatekeeper from sensing duplicate extensions.

To properly configure your Cisco Unified CME system to handle direct calls, call forwarding, and call transfers between Cisco Unified CME sites, make sure that you understand and configure the `dialplan-pattern` command. Also note that the mapping of public telephone numbers to internal extension numbers is not restricted to simple truncation of the digit string. Digit substitutions can be made using the `extension-pattern` keyword in the `dialplan-pattern` command, which is described in the “Dial-Plan Patterns” section on page 114. More sophisticated number manipulations can be managed with voice translation rules and voice translation profiles, which are described in the “Voice Translation Rules and Profiles” section on page 117.

In addition, your selection of a numbering scheme for phones that can be directly dialed from the PSTN is limited by your need to use the range of extensions that are assigned to you by the telephone company that provides your connection to the PSTN. For example, if your telephone company assigns you a range from 408-555-0100 to 408-555-0199, you may assign extension numbers only in the range 100 to 199 if those extensions are going to have Direct Inward Dialing (DID) access. For more information about DID, see the “Direct Inward Dialing” section on page 33.
Direct Inward Dialing

When you define an ephone-dn (extension number instance) using the `ephone-dn` command, the Cisco Unified CME system automatically creates a POTS dial peer with the ephone-dn endpoint as a destination. The default behavior is for the Cisco Unified CME system to create a single POTS dial peer for each ephone-dn. If the `dialplan-pattern` command is set and it matches against an ephone-dn number, two POTS dial peers are created, one for the local extension and one for the complete E.164 direct-dial telephone number. For example, an ephone-dn extension number is 1234 and the dial-plan pattern is “dialplan-pattern 1 4085551... extension-length 4.” One POTS dial peer is created for “1234” and a second POTS dial peer is created for “4085551234.” A third POTS dial peer is created if an ephone-dn secondary number is defined, and a fourth dial peer is created for this number if the secondary number also matches a dial-plan pattern. When the PSTN connects a DID call for “4085551234” to the Cisco Unified CME system, it also forwards the extension digits “1234” to allow the system to route the call. Dial peers that are created by the `ephone-dn` command can be viewed using the `show telephony-service dial-peer` command.

For more information about dial peers, refer to *Dial Peer Configuration on Voice Gateway Routers*.

PBX or Keyswitch Model

When setting up a Cisco Unified CME system, you need to decide if call handling should be similar to that of a PBX, similar to that of a keyswitch, or a hybrid of both. Cisco Unified CME provides a significant amount of flexibility in this area, but requires that you have a clear understanding of the model that you choose.

The simplest case is the PBX model, in which most of the IP phones in your system have a single unique extension number. Incoming PSTN calls are routed to a receptionist at an attendant console or to an automated attendant. Phone users may be in separate offices or be geographically separated and therefore often use the telephone to contact each other.

For this model, it is recommended that you configure ephone-dn entries to use the dual-line configuration option. With this setting, each button that appears on an IP phone can handle two concurrent calls. The phone user toggles between calls using the blue navigation button on the phone. Dual-line ephone-dn entries enable your configuration to support call waiting, call transfer with consultation, and three-party conferencing (G.711 only). If you assign strictly sequential extension numbers to newly registering IP phones, the Cisco Unified CME setup tool can assist you in creating a PBX-style configuration automatically.

*Figure 11* shows a PSTN call that is received at the Cisco Unified CME router, which sends it to the designated receptionist or automated attendant (1), which then routes it to the requested extension (2).
In a keyswitch type of system, you can set up most of your phones to have a nearly identical configuration, in which each phone is able to answer any incoming PSTN call on any line. Phone users are generally in close proximity and have little need to use the telephone to contact each other.

For example, a 3x3 keyswitch system has three PSTN lines shared across three telephones, such that all three PSTN lines appear on each of the three telephones. This permits an incoming call on any PSTN line to be directly answered by any telephone—without the aid of a receptionist, auto-attendant or the use of (expensive) DID lines. Also, the lines act as shared lines—a call can be put on hold on one phone and resumed on another phone without invoking call transfer.

In the keyswitch model, the same ephone-dn entries are assigned to all IP phones. When an incoming call arrives, it rings all available IP phones. When multiple calls are present within the system at the same time, each individual call (ringing or waiting on hold) is visible and can be directly selected by pressing the corresponding line button on an IP phone. In this model, calls can be moved between phones simply by putting the call on hold at one phone and selecting the call using the line button on another phone. In a keyswitch usage model, it is often not appropriate to use the ephone-dn dual-line option because the PSTN lines to which the ephone-dn entries correspond do not themselves support dual-line configuration. Use of the dual-line option also makes configuration of call-coverage (hunting) behaviors more complex.

You configure the keyswitch model by creating a set of ephone-dn entries that correspond one-to-one with your PSTN lines. Then you configure your PSTN ports to route incoming calls to those ephone-dns. The maximum number of PSTN lines that you can assign in this model might be limited by the number of available buttons on your IP phones. If so, the ephone-dn overlay option may be useful for extending the number of lines that can be accessed by a phone.

Figure 12 shows an incoming call from the PSTN (1), which is routed to extension 1001 on all three phones (2).
PBX and keyswitch configurations can be mixed on the same IP phone and can include both unique per-phone extensions for PBX-style calling and shared lines for keyswitch-style call operations. Single-line and dual-line ephone-dns can be combined on the same phone, and you can include an intercom ephone-dn for a dedicated voice path to another phone.

For example, you can design a 3x3 keyswitch system as shown in Figure 12 and then add another, unique extension on each phone (Figure 13). This setup will allow each phone to have a “private” line to use to call the other phones or to make outgoing calls.

**Figure 12**  **Incoming PSTN Call Using Keyswitch Model**

**Figure 13**  **Incoming PSTN Call Using Hybrid PBX-Keyswitch Model**

**Additional References**

- Related Documents, page 36
- Standards, page 37
- MIBs, page 38
- RFCs, page 38
### Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Unified CallManager Express documentation</td>
<td><em>Cisco Unified CME Documentation Roadmap</em></td>
</tr>
<tr>
<td>Cisco Unified CME Basic Automatic Call Distribution (B-ACD) and Auto-Attendant (AA) service</td>
<td><em>Cisco Unified CME B-ACD and Tcl Call-Handling Applications</em></td>
</tr>
<tr>
<td>Cisco IOS software command references</td>
<td><em>Cisco IOS Software Releases 12.4 Mainline Command References</em></td>
</tr>
<tr>
<td></td>
<td><em>Cisco IOS Debug Command Reference, Release 12.4</em></td>
</tr>
<tr>
<td></td>
<td><em>Cisco IOS Security Command Reference, Release 12.4</em></td>
</tr>
<tr>
<td></td>
<td><em>Cisco IOS Voice Command Reference</em></td>
</tr>
<tr>
<td></td>
<td><em>Cisco Unified CallManager Express (All Versions) Command Reference</em></td>
</tr>
<tr>
<td>Cisco IOS software configuration guides</td>
<td><em>Cisco IOS Voice Configuration Library</em></td>
</tr>
<tr>
<td></td>
<td><em>Cisco IOS Software Releases 12.4 Mainline Configuration Guides</em></td>
</tr>
<tr>
<td>Cisco IOS voice troubleshooting information</td>
<td><em>Cisco IOS Voice Troubleshooting and Monitoring Guide</em></td>
</tr>
<tr>
<td>Dial peers, DID, and other dialing issues</td>
<td><em>Dial Peer Configuration on Voice Gateway Routers</em></td>
</tr>
<tr>
<td></td>
<td><em>Understanding One Stage and Two Stage Dialing</em> (technical note)</td>
</tr>
<tr>
<td></td>
<td><em>Understanding How Inbound and Outbound Dial Peers Are Matched on Cisco IOS Platforms</em> (technical note)</td>
</tr>
<tr>
<td></td>
<td><em>Using IOS Translation Rules - Creating Scalable Dial Plans for VoIP Networks</em> (sample configuration)</td>
</tr>
<tr>
<td>Dynamic Host Configuration Protocol (DHCP)</td>
<td>“DHCP” part of the <em>Cisco IOS IP Addressing Services Configuration Guide</em></td>
</tr>
<tr>
<td>Fax and modem configurations</td>
<td><em>Cisco IOS Fax and Modem Services over IP Application Guide</em></td>
</tr>
<tr>
<td>FXS ports</td>
<td><strong>FXS Ports in H.323 Mode</strong></td>
</tr>
<tr>
<td></td>
<td>“Configuring Analog Voice Ports” section of the <em>Cisco IOS Voice Port Configuration Guide</em></td>
</tr>
<tr>
<td></td>
<td>Caller ID</td>
</tr>
<tr>
<td></td>
<td><em>Cisco IOS Fax and Modem Services over IP Application Guide</em></td>
</tr>
<tr>
<td>FXS Ports in SCCP Mode on Cisco VG 224 Analog Phone Gateway</td>
<td><em>SCCP Controlled Analog (FXS) Ports with Supplementary Features in Cisco IOS Gateways</em></td>
</tr>
<tr>
<td></td>
<td>Cisco VG 224 Analog Phone Gateway data sheet</td>
</tr>
<tr>
<td>H.323</td>
<td><em>Cisco IOS H.323 Configuration Guide</em></td>
</tr>
<tr>
<td>Network management software using Cisco Packet Telephony Center - Virtual Switch (Cisco PTC - VS)</td>
<td><em>Provisioning Manager - Managed Cisco CallManager Express Routers</em></td>
</tr>
</tbody>
</table>
Cisco Unified CallManager Express Overview

---

## Additional References

### Related Websites

**Related Topic**

1. Network Time Protocol (NTP)
   - “Performing Basic System Management” chapter of *Cisco IOS Network Management Configuration Guide*

2. Phone documentation for Cisco phones
   - Cisco 7900 Series IP Phones
   - Cisco ATA 180 Series Analog Telephone Adaptors
   - Cisco IP Communicator

3. Phone documentation for Cisco Unified CME
   - Quick Reference Cards
   - User Guides

4. Public key infrastructure (PKI)
   - “Part 5: Implementing and Managing a PKI” in the *Cisco IOS Security Configuration Guide*

5. SIP
   - *Cisco IOS SIP Configuration Guide*

6. TAPI and TSP documentation
   - See links at *Cisco Unified CME Documentation Roadmap*

7. Tcl IVR and VoiceXML
   - *Cisco IOS Tcl IVR and VoiceXML Application Guide - 12.3(14)T and later*
   - Default Session Application Enhancements
   - *Tcl IVR API Version 2.0 Programmer’s Guide*
   - *Cisco VoiceXML Programmer’s Guide*

8. VLAN class-of-service (COS) marking
   - *Enterprise QoS Solution Reference Network Design Guide*

9. Voice-mail integration
   - *Cisco Unified CallManager Express 3.0 Integration Guide for Cisco Unity 4.0*
   - *Integrating Cisco CallManager Express with Cisco Unity Express*

10. XML
    - *XML Provisioning Guide for Cisco CME/SRST*
    - *Cisco IP Phone Services Application Development Notes*

---

### Standards

**Standards**

- No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.

---

Related Topic Title and Location

- Cisco IOS configuration examples

  **Note**  
  From the website, select a technology category and subsequent hierarchy of subcategories, then click Technical Documentation > Configuration Examples.

---

Cisco Unified CallManager Express System Administrator Guide  |  37
### MIBs

<table>
<thead>
<tr>
<th>MIBs</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>CISCO-CCME-MIB</td>
<td></td>
</tr>
<tr>
<td>MIB CISCO-VOICE-DIAL-CONTROL-MIB</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

### RFCs

<table>
<thead>
<tr>
<th>RFCs</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.</td>
<td>—</td>
</tr>
</tbody>
</table>
Prerequisites and Restrictions

Cisco Unified CallManager Express (Cisco Unified CME) has certain system prerequisites and restrictions, which are described in this chapter. This chapter contains the following sections:

- Prerequisites, page 39
- Restrictions, page 41

Note
Prior to version 4.0, the name of this product was Cisco CallManager Express (Cisco CME). Prior to version 3.0, the name was Cisco IOS Telephony Services (Cisco ITS).

Note

Prerequisites

Prerequisites for installing Cisco Unified CallManager Express are grouped into the following categories:

- License Prerequisites, page 40
- Memory Prerequisites, page 40
- Network Prerequisites, page 40
License Prerequisites

You must purchase a base Cisco Unified CME feature license and phone user licenses that entitle you to use Cisco Unified CME.

Note

To support H.323 call transfers and forwards to network devices that do not support the H.450 standard, such as Cisco Unified CallManager, a tandem gateway is required in the network. The tandem gateway must be running Cisco IOS software 12.3(7)T or later and requires the Integrated Voice and Video Services feature license (FL-GK-NEW-xxx), which includes H.323 gatekeeper, IP-to-IP gateway, and H.450 tandem functionality.

Memory Prerequisites

- For information about the maximum number of Cisco Unified IP phones, maximum number of directory numbers (ephone-dns) or virtual voice ports, and memory requirements for Cisco Unified CME, find the Cisco Unified CallManager Express Supported Firmware, Platforms, Memory, and Voice Products for your Cisco Unified CME release. A link to this document can be found in the Cisco Unified CME Document Roadmap.
- Disable Smartinit and allocate ten percent of the total DRAM to support Cisco Unified CME with the following command:

  ```
  Router(config)# memory-size iomem 10
  ```

Network Prerequisites

- IP routing must be enabled.
- VoIP networking must be operational. For quality and security purposes, it is recommended to have separate virtual LANs (VLANs) for data and voice. The IP network assigned to each VLAN should be large enough to support addresses for all nodes on that VLAN. Cisco Unified CME phones receive their IP addresses from the voice network, whereas all other nodes such as PCs, servers, and printers receive their IP addresses from the data network.
- The voice VLAN should be configured to receive IP addresses from a Dynamic Host Configuration Protocol (DHCP) server. A DHCP server for Cisco Unified CME phones is designated during Cisco Unified CME setup. For more information, see the “Task 4: Defining Network Settings” section on page 52.
- The clock on the router must be configured to the proper date and time. All Cisco Unified IP phones connected to the router will receive their time and date settings from the router clock. To keep the router clock accurate, configure the router for Network Time Protocol (NTP). For more information, see the “Task 4: Defining Network Settings” section on page 52.
- Trivial File Transfer Protocol (TFTP) must be enabled on the router to allow IP phones to download phone firmware files.
Restrictions

Restrictions for special types of call transfer are listed in the “Transfer and Forwarding Support” chapter.

Restrictions for Cisco Unified CME are grouped into the following categories:

- **General Phone Support Restrictions**, page 41
- **Analog Phone Support Restrictions**, page 41
- **Remote SCCP Phone Support Restrictions**, page 42
- **General Cisco Unified CME Restrictions**, page 42

### General Phone Support Restrictions

- No more Cisco Unified IP phones or extension numbers than the maximum specified in the *Cisco Unified CallManager Express Supported Firmware, Platforms, Memory, and Voice Products* for your Cisco Unified CME release. A link to this document can be found in the *Cisco Unified CME Documentation Roadmap*.
- The only platforms and phone devices supported are those that are listed in the *Cisco Unified CallManager Express Supported Firmware, Platforms, Memory, and Voice Products* for your Cisco Unified CME release. A link to this document can be found in the *Cisco Unified CME Documentation Roadmap*.
  - First-generation Cisco IP phones, such as the Cisco IP Phone 30 VIP and the Cisco IP Phone 12 SP+, are not supported.
  - The Cisco IP Phone 7970G and 7971G-GE do not support user and network localization. The *user-locale* and *network-locale* commands must be set to their default, United States (US).
  - IP phones connected to Cisco Unified CME systems require the use of out-of-band dual-tone multifrequency (DTMF) relay to transport DTMF (keypad) digits across VoIP connections. For more information, see the “Configuring DTMF Relay for H.323 Networks” section on page 59.

### Analog Phone Support Restrictions

- Cisco Unified CME features such as call forward and call park are not available for analog phones connected to FXS ports in H.323 mode. In order to support these features, SCCP supplementary features must be enabled on the FXS ports. For information about SCCP supplementary features, see the “Analog Phones” section on page 138 and the *Cisco Unified CME data sheet*.

FXS ports on platforms that cannot enable SCCP supplementary features can use H.323 mode to support call waiting, caller ID, hookflash transfer, modem pass-through, fax (T.38, Cisco fax relay, and pass-through), and PLAR. These features are provisioned as Cisco IOS voice features and not as Cisco Unified CME features. Note that when using Cisco Unified CME, you can configure FXS ports in H.323 mode for call waiting or hookflash transfer, but not both at the same time.

The following links provide information on analog phone features for FXS ports in H.323 mode:
  - “Configuring Analog Voice Ports” section in the *Voice Port Configuration Guide*
  - “Caller ID” section of the *Cisco IOS Voice Configuration Library*
  - *Cisco IOS Fax and Modem Services over IP Application Guide*
**Remote SCCP Phone Support Restrictions**

Remote skinny client control protocol (SCCP) phones connected across WAN links are subject to the following restrictions:

- Cisco TAC will not handle any voice or signaling issues for remote IP phones, unless the same issue can be replicated for LAN phones.
- E911 or emergency calls are not supported from remote IP phones.
- All calls made to and from remote IP phones must use G.711. Cisco Unified CME does not support the ability to specify G.729 codec for remote IP phones.
- For inbound or outbound calls, remote IP phones cannot fail and go over to a PSTN connection. Remote phones must use the WAN for all calls, even if available bandwidth is not sufficient to guarantee voice quality.
- Remote IP phones do not support Network Address Translation (NAT). All Cisco Unified CME phones must use IP addresses that are can be routed to and from Cisco Unified CME. Remote IP phones must be able to access the IP addresses that are used for all other local and remote phones.
- All PSTN access is through the central site only. PSTN termination at the remote site is not supported.
- Cisco Unified CME does not support Call Admission Control (CAC) for remote SCCP phones, so voice quality can degrade if a WAN link is oversubscribed. High-bandwidth data applications used over a WAN can cause degradation of voice quality for remote IP phones.

**General Cisco Unified CME Restrictions**

- Cisco Unified CME cannot register as a member of a Cisco Unified CallManager cluster.
- The only codecs supported are G.711 and G.729. For conferencing and music on hold (MOH) support with G.729, hardware digital signal processors (DSPs) are required for transcoding G.729 between G.711.
- Once a three-way conference has been established, a participant cannot use call transfer to join the remaining conference participants to a different number.
- Cisco Unified CME does not support the following:
  - CiscoWorks IP Telephony Environment Monitor (ITEM)
  - Element Management System (EMS) integration
  - Media Gateway Control Protocol (MGCP) on-net calls
  - Java Telephony Application Programming Interface (JTAPI) applications, such as the Cisco IP Softphone, IPCC, or IPCC Express, Cisco Unified CallManager Auto Attendant or Cisco Personal Assistant
  - Telephony Application Programming Interface (TAPI) Version 2.1. Cisco Unified CME implements only a small subset of TAPI functionality. It does support operation of multiple independent clients (for example, one client per phone line), but not full support for multiple-user or multiple-call handling, which is required for complex features such as automatic call distribution (ACD) and Cisco Unified Contact Center (formerly Cisco IPCC). Also, this TAPI version does not have direct media- and voice-handling capabilities.
- Cisco Voice Manager (CVM) does not support IP phone configurations.
Installing Cisco Unified CME

This chapter explains how to install Cisco Unified CallManager Express (Cisco Unified CME). It contains the following sections:

- Installation Tasks Overview, page 44
- Task 1: Installing Hardware, page 45
- Task 2: Downloading Cisco IOS Software, page 46
- Task 3: Downloading Cisco Unified CME Software, page 46
- Task 4: Defining Network Settings, page 52
- Task 5: Setting Cisco Unified CME Parameters, page 60
- Task 6: Provisioning Phones, page 70
- Task 7: Plugging in Phones, page 76
- Task 8: Resetting and Restarting Phones, page 76
- Task 9: Configuring Call Flows, page 81
- Task 10: Adding Features, page 81
- Task 11: Configuring Security for Phones, page 82
- Task 12: Configuring Support for Multi-Site Functionality, page 82
- Verifying the Cisco Unified CME Configuration, page 83
- Configuration Examples, page 86

Note
Prior to version 4.0, the name of this product was Cisco CallManager Express (Cisco CME). Prior to version 3.0, the name was Cisco IOS Telephony Services (Cisco ITS).

Note
Installation Tasks Overview

This chapter provides details about installation tasks. Table 15 contains a checklist that describes when to perform each task, what happens during the task, and what result you should expect when you complete the task.

Note

You can use the Cisco IPC Express Quick Configuration Tool (QCT) to automatically set up phones if you are using a shared DHCP address pool for your phones. If you use QCT, you do not have to perform Task 4: Defining Network Settings, Task 5: Setting Cisco Unified CME Parameters, or Task 6: Provisioning Phones as described in this chapter.

See Installing Cisco IPC Express: Cisco CallManager Express and Cisco Unity Express.

Table 15  Cisco Unified CME Installation Tasks Checklist

<table>
<thead>
<tr>
<th>Installation Task</th>
<th>When to Perform the Task</th>
<th>Description</th>
<th>Result of Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>Task 1: Installing Hardware</td>
<td>For a new site or new hardware installation.</td>
<td>Installs appropriate hardware.</td>
<td>Router is up and running.</td>
</tr>
<tr>
<td>Task 2: Downloading Cisco IOS Software</td>
<td>For an upgraded site or new site without pre-installed software.</td>
<td>Downloads and installs appropriate Cisco IOS software.</td>
<td>Correct Cisco IOS software is installed.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Network communication is enabled.</td>
</tr>
<tr>
<td>Task 3: Downloading Cisco Unified CME Software</td>
<td>For an upgraded site or new site without pre-installed software.</td>
<td>Downloads appropriate software and makes it available to Cisco Unified CME.</td>
<td>Cisco Unified CME software is installed.</td>
</tr>
<tr>
<td>Task 4: Defining Network Settings</td>
<td>When a site needs to be connected to a network or network addresses change.</td>
<td>Sets up a DHCP server and NTP, which Cisco Unified CME requires.</td>
<td>DHCP is set up.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>NTP is set up.</td>
</tr>
<tr>
<td>Task 5: Setting Cisco Unified CME Parameters</td>
<td>For an upgraded or new site.</td>
<td>Defines basic information about this Cisco Unified CME system.</td>
<td>Basic Cisco Unified CME settings are made, such as maximum number of phones and IP address.</td>
</tr>
<tr>
<td>Task 6: Provisioning Phones</td>
<td>For an upgraded or new site.</td>
<td>Creates ephone-dns and allots ephone-dns to phones.</td>
<td>Phones have received their assigned extensions.</td>
</tr>
<tr>
<td>Task 7: Plugging in Phones</td>
<td>For an upgraded or new site.</td>
<td>Connects physical instruments to the system.</td>
<td>Phones have dial tone.</td>
</tr>
<tr>
<td>Task 8: Resetting and Restarting Phones</td>
<td>Whenever changing a setting or feature related to a phone or configuration file.</td>
<td>Reboots phones so that they pick up new configuration information.</td>
<td>Phones have been reset or restarted to receive configuration files and can make and receive basic calls</td>
</tr>
</tbody>
</table>

Make sure that you have the correct hardware and that your IP network is functioning correctly. Refer to documentation for your particular hardware and to the “Installing Hardware and Software” chapter of *Installing Cisco IPC Express: Cisco CallManager Express and Cisco Unity Express*. 

### Table 15  
**Cisco Unified CME Installation Tasks Checklist**

<table>
<thead>
<tr>
<th>Installation Task</th>
<th>When to Perform the Task</th>
<th>Description</th>
<th>Result of Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>Task 9: Configuring Call Flows</td>
<td>For upgraded or new sites or when calling patterns change.</td>
<td>Sets up</td>
<td>• Dial plans and voice translation rules are established.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Call-coverage and call-handling features are configured.</td>
</tr>
<tr>
<td>Task 10: Adding Features</td>
<td>Whenever a feature needs to be added or changed.</td>
<td>Sets up Cisco Unified CME GUI support, phone support and features, voice mail, and system features such as directories, music on hold, and so forth.</td>
<td>• Cisco Unified CME GUI is set up.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Features have been added and verified.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Interoperability with a voice-mail system is established.</td>
</tr>
<tr>
<td>Task 11: Configuring Security for Phones</td>
<td>When a more secure system is desired.</td>
<td>Sets up secure SCCP signaling between Cisco Unified CME and IP phones and disallows automatic phone registration.</td>
<td>• Phone authentication is configured.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Automatic registration is blocked, if desired.</td>
</tr>
<tr>
<td>Task 12: Configuring Support for Multi-Site Functionality</td>
<td>Whenever a particular kind of support needs to be added or changed to operate over several sites.</td>
<td>Sets up support for multiple Cisco Unified CME sites to work together.</td>
<td>As needed:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• DTMF relay is set up.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Transfer and forwarding options are set up.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Transcoding resources are configured.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Teleworker remote phones are established.</td>
</tr>
<tr>
<td>Verifying the Cisco Unified CME Configuration</td>
<td>Whenever a change is made to the router configuration.</td>
<td>Checks that settings in the router configuration are correct.</td>
<td>• Router configuration is correct.</td>
</tr>
</tbody>
</table>
Task 2: Downloading Cisco IOS Software

Download and install the appropriate IP VOICE image from the Cisco Software Center. Consult the following sources to determine the correct Cisco IOS software version:

- Feature Navigator at the following URL: http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp
- Cisco Unified CallManager Express Supported Firmware, Platforms, Memory, and Voice Products for your Cisco Unified CME release. See links for this document at the following URL: http://www.cisco.com/en/US/products/sw/voicesw/ps4625/products_documentation_roadmap09186a0080189132.html

Task 3: Downloading Cisco Unified CME Software

For Cisco Unified CME, certain files must be downloaded and installed in the Cisco Unified CME router flash memory. The files and the process are discussed in the following sections:

- Cisco Unified CME Files, page 46
- Downloading Cisco Unified CME Software, page 48
- Upgrading Individual Phone Firmware Files, page 50

Note

If you are downgrading or upgrading Cisco Unified CME and use the Cisco Unified CME GUI, you must be sure to also downgrade or upgrade GUI files. For more information, see the “GUI Files” section on page 47.

Note

Customers who purchase a router bundle enabled with Cisco Unified CME will have the necessary Cisco Unified CME files installed at time of manufacture.

Cisco Unified CME Files

This section contains a list of the files that are used with Cisco Unified CME. The files listed in this section are included in zipped or tar archives that can be downloaded from the Cisco Unified CME software download website at http://www.cisco.com/cgi-bin/tablebuild.pl/ip-iostsp. Descriptions of the files are grouped into the following categories:

- Basic Files, page 47
- GUI Files, page 47
- Phone Firmware Files, page 47
- XML Template, page 48
- Music-on-Hold (MOH) File, page 48
- Script Files, page 48
- Bundled TSP Archive, page 48
Basic Files

A tar archive contains the basic files you need for Cisco Unified CME. Be sure to download the correct version for the Cisco IOS software release that is running on your router. To install basic files, see the “Downloading Cisco Unified CME Software” section on page 48.

The basic tar archive generally also contains the phone firmware files that you require, although you may occasionally need to download individual phone firmware files. To install individual phone firmware files, see the “Upgrading Individual Phone Firmware Files” section on page 50.

GUI Files

A tar archive contains the files that you need to use the Cisco Unified CME graphical user interface (GUI), which provides a mouse-driven interface for provisioning phones after basic installation is complete. To install GUI files, see the “Downloading Cisco Unified CME Software” section on page 48.

Note

Cisco Unified CME GUI files are version-specific; GUI files for one version of Cisco Unified CME are not compatible with any other version of Cisco Unified CME. When downgrading or upgrading Cisco Unified CME, the GUI files for the old version must be overwritten with GUI files that match the Cisco Unified CME version that is being installed.

Phone Firmware Files

Phone firmware files provide code to enable phone displays and operations. These files are specialized for each phone type and are periodically revised. You must be sure to have the appropriate phone firmware files for the types of phones and Cisco Unified CME version you have at your site.

New IP phones are shipped from Cisco with a default manufacturing image. IP Phones running manufacturing phone firmware may not function properly when registered to Cisco Unified CME and therefore must be upgraded to a phone firmware version supported by Cisco Unified CME. By following the instructions in the “Upgrading Individual Phone Firmware Files” section on page 50, you can upgrade IP phones from the firmware that was installed during manufacture to a phone firmware version that is supported by Cisco Unified CME.

There may be one or more firmware files for each phone type. There may be signed and unsigned versions of the files available. Signed versions are recommended if your version of Cisco Unified CME supports them. Signed binary files have .sbn file extensions, and unsigned files have .bin file extensions.

Note

The phone version is derived from the final eight digits of the phone firmware filename. For example, [P00307020300] is phone version 7.2(3.0).

The phone firmware filenames for each phone type and Cisco Unified CME version are listed in the Cisco CallManager Express Supported Firmware, Platforms, Memory, and Voice Products. Find links to this document in the Cisco Unified CME Documentation Roadmap.

Generally, phone firmware files are included in the Cisco Unified CME software archive that you download, but they can also be posted on the software download website as individual files or archives.

Install only the firmware files needed for the types of phones that you have at your site. To install files from an archive, see the “Task 3: Downloading Cisco Unified CME Software” section on page 46. To install individual firmware files or upgrade to signed versions of files, see the “Upgrading Individual Phone Firmware Files” section on page 50.
XML Template

The file called xml.template can be copied and modified to allow or restrict specific GUI functions to customer administrators, a class of administrative users with limited capabilities in a Cisco Unified CME system. This file is included in both tar archives (cme-basic-... and cme-gui-...). To install the file, see the “Downloading Cisco Unified CME Software” section on page 48.

Music-on-Hold (MOH) File

An audio file named music-on-hold.au provides music for external callers on hold when a live feed is not used. This file is included in the tar archive with basic files (cme-basic-...). To install the file, see the “Downloading Cisco Unified CME Software” section on page 48.

Script Files

Archives containing Tcl script files are listed individually on the Cisco Unified CME software download website. For example, the file named app-h450-transfer.2.0.0.9.zip.tar contains a script that adds H.450 transfer and forwarding support for analog FXS ports. To install an archive, see the “Downloading Cisco Unified CME Software” section on page 48.

The Cisco Unified CME Basic Automatic Call Distribution and Auto Attendant Service (B-ACD) requires a number of script files and audio files, which are contained in a tar archive with the name cme-b-acd-.... For a list of files in the archive and for more information about the files, see the Cisco Unified CallManager Express B-ACD and TCL Call-Handling Applications document for your release. For a link to this document, see the Cisco Unified CME Documentation Roadmap. For information about installing an archive, see the “Downloading Cisco Unified CME Software” section on page 48.

Bundled TSP Archive

An archive is available at the Cisco Unified CME software download website that contains several Telephony Application Programming Interface (TAPI) Telephony Service Provider (TSP) files. These files are needed to set up individual PCs for Cisco Unified IP phone users who wish to make use of Cisco Unified CME-TAPI integration with TAPI-capable PC software. To install the files from the archive, see the installation instructions in the TSP documentation. For links to the TSP documentation, see the Cisco Unified CME Documentation Roadmap.

Downloading Cisco Unified CME Software

This procedure installs Cisco Unified CME files from the Cisco Unified CME software download website at http://www.cisco.com/cgi-bin/tablebuild.pl/ip-iostsp.

As described in the “Cisco Unified CME Files” section on page 46, there are a number of different types of files available at the Cisco Unified CME software download website. Most of the files are archives that need to be uncompressed before individual files can be copied to the router. In general, the following file-naming conventions apply to files on the Cisco Unified CME software download website:

- cme-basic-...—Basic Cisco Unified CME files, including phone firmware files for a particular Cisco Unified CME version or versions.
- cme-gui-...—Files required for the Cisco Unified CME GUI.
- cmterm..., P00..., 7970...—Phone firmware files.
- cme-b-acd...—Files required for Cisco Unified CME B-ACD service.
Files required for TAPI applications are not included in the tar archive. To install these files, download the TAPI files separately and follow the installation instructions in the Cisco IOS TSP documentation. For a link to the Cisco IOS TSP documentation, see the Cisco Unified CME Documentation Roadmap.

Examples in this section may use software version numbers that were current when this document was written. You should use the latest software version that is available on the software download site.

**SUMMARY STEPS**

1. Download the desired archive or file to a TFTP server that is accessible to the Cisco Unified CME router.
2. Uncompress and copy each archive to router flash memory, except for phone firmware files.
3. Copy to router flash memory only the firmware files for phone types that you have at your site and allow TFTP access for them.

**DETAILED STEPS**

**Step 1** Download the desired archive or file to a TFTP server that is accessible to the Cisco Unified CME router.

The Cisco Unified CME software download site is located at http://www.cisco.com/cgi-bin/tablebuild.pl/ip-iostsp.

**Step 2** Uncompress and copy each archive to router flash memory, except for phone firmware files.

- If the archive is a tar archive, use the `archive tar` command:
  
  ```
  Router# archive tar /xtract source-url flash:/file-url
  ```

  For example, to extract contents of cme-basic-123-11T.tar from TFTP server 192.168.1.1 to router flash memory, use this command:

  ```
  Router# archive tar /xtract tftp://192.168.1.1/cme-basic-123_11T.tar flash:
  ```

- If the archive is a Winzip file, use the WinZip program to uncompress the file and the copy command to copy the files to router flash:

  ```
  Router# copy tftp://x.x.x.x/P00307020300.sbn flash:
  ```

For more information about copying files to flash memory, see “Copying Images from a Network Server to Flash Memory.”

**Step 3** Copy to router flash memory only the firmware files for phone types that you have at your site and allow TFTP access for them.

- Consult the Cisco CallManager Express Supported Firmware, Platforms, Memory, and Voice Products for your Cisco Unified CME version to find out the names of the phone firmware files you need to install for the types of phones that you have at your site and the version of Cisco Unified CME software that you are installing. To find this document for your Cisco Unified CME version, use the links in the Cisco Unified CME Documentation Roadmap.

- If the files you need were included in the basic archive that you downloaded, use the `copy` command to copy them to router flash memory and the `tftp-server` command to make the files available to phones via TFTP.
Installing Cisco Unified CME

Task 3: Downloading Cisco Unified CME Software

50

Cisco Unified CallManager Express System Administrator Guide

Router> enable
Router# copy tftp://x.x.x.x/P00307020300.sbn flash:
Router# configure terminal
Router (config)# tftp-server flash:P00307020300.sbn

c. If the files you need were not in the basic archive, go to the Cisco Unified CME software download website and download the files individually. Then copy them to router flash memory and make them available through TFTP as explained in Step 3 b.

Note At this stage of the installation, phones do not yet have their phone firmware installed. The firmware files must first be loaded in the system using the load command, and the phones must be reset in order to download the firmware. These steps are part of the following tasks that are described later in this chapter: “Task 5: Setting Cisco Unified CME Parameters” section on page 60 and “Task 8: Resetting and Restarting Phones” section on page 76.

Step 4 Proceed to the “Task 4: Defining Network Settings” section on page 52.

Upgrading Individual Phone Firmware Files

The previous procedure explained how to install phone firmware files as part of a general Cisco Unified CME installation or upgrade. There may be occasions, however, when you need to upgrade individual phone firmware files without upgrading Cisco Unified CME software.

For example, you might have installed unsigned files and later find out that signed files are available. Some Cisco Unified IP phones can use either of two types of firmware images: signed or unsigned images. Signed binary files support image authentication, which increases system security. Signed images have an .sbn extension, while unsigned images have a .bin extension. If you are using a version of Cisco Unified CME that supports signed firmware files, it is recommended that you use signed files.

Note The phone version is derived from the final eight digits of the phone firmware filename. For example, [P00307020300] is phone version 7.2(3.0).

This procedure explains how to upgrade the phone firmware for a particular type of phone.

SUMMARY STEPS

1. Determine the phone firmware that the phone type is currently using.
2. Disable TFTP file sharing for the current phone firmware and remove the file from flash.
3. Copy the new phone firmware to router flash.
4. Enable TFTP file sharing for the new phone firmware.
5. Load the new phone firmware.
6. Reset phones.
7. Exit to privileged EXEC mode and verify that phones are using the new phone firmware.
DETAILED STEPS

**Step 1**  Determine the phone firmware that the phone type is currently using.

a. Use the **show telephony-service all** command to determine the phone firmware that each type of phone is currently using. In this example, the filename is P00307020300 and the version is 7.2(3.0).

```
Router# show telephony-service all

CONFIG (Version=4.0(0))
=====================  
Version 4.0(0)  
Cisco Unified CallManager Express 
For on-line documentation please see:  
ip source-address 172.16.2.211 port 2000  
load 7960-7940 P00307020300
```

b. Use the **show flash:** command to learn the filenames associated with that phone firmware

```
Router# show flash:

31  128996 Sep 19 2005 12:19:02 -07:00 P00307020300.bin
32   461 Sep 19 2005 12:19:02 -07:00 P00307020300.loads
33  681290 Sep 19 2005 12:19:04 -07:00 P00307020300.sb2
34  129400 Sep 19 2005 12:19:04 -07:00 P00307020300.sbn
```

**Step 2**  Disable TFTP file sharing for the current phone firmware and remove the files from flash.  
This step is optional but it is a good housekeeping practice.

```
Router (config)# no tftp-server flash:P00307020300.bin
```

**Step 3**  Copy the new phone firmware to router flash.

```
Router# copy tftp://x.x.x.x/P00307020300.sbn flash:
```

**Step 4**  Enable TFTP file sharing for the new phone firmware.

```
Router# configure terminal  
Router(config)# tftp-server flash:P00307020300.loads  
Router(config)# tftp-server flash:P00307020300.sb2  
Router(config)# tftp-server flash:P00307020300.sbn  
Router(config)# tftp-server flash:P00307020300.bin
```

**Step 5**  Load the new phone firmware.  
Note that no file extension is used for the argument in this command.

```
Router (config)# telephony-service  
Router (config-telephony)# load 7960-7940 P00307020300
```

**Step 6**  Reset phones.

```
Router(config-telephony)# reset all
```

**Step 7**  Exit to privileged EXEC mode and verify that phones are using the new phone firmware.

```
Router(config-telephony)# exit  
Router(config)# exit  
Router# show ephone phone-load
```
Task 4: Defining Network Settings

The procedures in this section define settings that enable Cisco Unified CME to work with your network. You may not need to perform these procedures, but they are included here for ease of use.

- **Defining a DHCP Service**, page 52 (Required only if you do not have an existing DHCP server on the LAN)
- **Changing the TFTP Server Address**, page 57 (Required only when changing the TFTP server address)
- **Setting Network Time Protocol**, page 57 (Required only if it has not been previously set)
- **Configuring DTMF Relay for H.323 Networks**, page 59 (Required only for multi-site installations)

---

**Note**

You can store phone configuration files on an external TFTP server, and you can generate configuration files for each phone or phone type to support alternative user and network locales. For more information, see the “Configuration File Support” section on page 91.

---

**Note**

VLAN CoS marking—Cisco Unified CME 4.0 and later releases no longer automatically process Layer-3-to-Layer-2 VLAN Class of Service (CoS) priority marking. If you need to configure L3-to-L2 marking, you can do so on the Cisco Unified CME router, as explained in the Enterprise QoS Solution Reference Network Design Guide.

Cisco Unified CME will continue to mark Layer 3, but Layer 2 marking is now only handled in the Cisco IOS software. Any Quality of Service (QoS) design that requires Layer 2 marking will have to be explicitly configured, either on a Catalyst switch that supports this capability or on the Cisco Unified CME router under the Ethernet interface configuration.

For more information, see the Enterprise QoS Solution Reference Network Design Guide.

---

**Defining a DHCP Service**

---

**Note**

DHCP setup is not required if you already have a DHCP server on the LAN that can be used to provide addresses to the Cisco Unified CME phones. Proceed to the “Setting Network Time Protocol” section on page 57.

---

**Note**

If you are using the Cisco IPC Express Quick Configuration Tool (QCT) to configure phones and you need just one DHCP IP address pool, the QCT will create the address pool for you. You do not have to perform the steps in this section. Proceed to the “Setting Network Time Protocol” section on page 57.

---

When a Cisco Unified IP phone is connected to the Cisco Unified CME system, it automatically queries for a Dynamic Host Configuration Protocol (DHCP) server. The DHCP server responds by assigning an IP address to the Cisco Unified IP phone and providing the IP address of the TFTP server through DHCP option 150. Then the phone registers with the Cisco Unified CME server and attempts to get configuration and phone firmware files from the TFTP server.
Choose one of the following tasks to set up DHCP service for your IP phones:

- If your Cisco Unified CME router is the DHCP server and you can use a single shared address pool for all your DHCP clients, use the “Defining a Single DHCP IP Address Pool” section on page 53.
- If your Cisco Unified CME router is the DHCP server and you need separate pools for non-IP-phone DHCP clients, use the “Defining a Separate DHCP IP Address Pool for Each Cisco Unified IP Phone” section on page 54.
- If the Cisco Unified CME router is not the DHCP server and you want to relay DHCP requests from IP phones to a DHCP server on a different router, use the “Defining a DHCP Relay Server” section on page 56.

For more information about DHCP, see the “DHCP” part of the Cisco IOS IP Addressing Services Configuration Guide.

**Note**

If you need to change the address of the TFTP server after you have initially defined it, refer to the instructions in the “Changing the TFTP Server Address” section on page 57.

### Defining a Single DHCP IP Address Pool

This task creates a shared pool of IP addresses, in which all DHCP clients receive the same information, including the option 150 TFTP server IP address. The benefit of selecting this method to set up DHCP service is that you set up only one DHCP pool. However, this method will not be adequate if some (non-IP-phone) clients need to use a different TFTP server address.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. ip dhcp pool pool-name
4. network ip-address [mask /prefix-length]
5. option 150 ip ip-address
6. default-router ip-address

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>
## Task 4: Defining Network Settings

### Defining a Separate DHCP IP Address Pool for Each Cisco Unified IP Phone

This task creates a name for a DHCP server address pool and specifies IP and MAC addresses. This method requires that you make an entry for every IP phone.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `ip dhcp pool pool-name`
4. `host ip-address subnet-mask`
5. `client-identifier mac-address`
6. `option 150 ip ip-address`
7. `default-router ip-address`

---

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 3</strong> <code>ip dhcp pool pool-name</code></td>
<td>Creates a name for the DHCP server address pool and enters DHCP pool configuration mode.</td>
</tr>
</tbody>
</table>
| **Example:** 
  `Router(config)# ip dhcp pool mypool` | |
| **Step 4** `network ip-address [mask | /prefix-length]` | Specifies the IP address of the DHCP address pool and the optional mask or number of bits in the address prefix, preceded by a forward slash. |
| **Example:** 
  `Router(config-dhcp)# network 10.0.0.0 255.255.0.0` | |
| **Step 5** `option 150 ip ip-address` | Specifies the TFTP server address from which the Cisco Unified IP phone downloads the image configuration file. This is your Cisco Unified CME router address. |
| **Example:** 
  `Router(config-dhcp)# option 150 ip 10.0.0.1` | |
| **Step 6** `default-router ip-address` | (Optional) Specifies the router that the IP phones will use to send or receive IP traffic that is external to their local subnet. |
| **Example:** 
  `Router(config-dhcp)# default-router 10.0.0.1` | If the Cisco Unified CME router is the only router on the network, this address should be the Cisco Unified CME IP source address. This command can be omitted if IP phones need to send or receive IP traffic only to or from devices on their local subnet. The IP address that you specify for default router will be used by the IP phones for fallback (Survivable Remote Site Telephony or SRST) purposes. If the Cisco Unified CME IP source address becomes unreachable, IP phones will attempt to register to the address specified in this command. |
### INSTALLING CISCO UNIFIED CME

#### TASK 4: DEFINING NETWORK SETTINGS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
  - Enter your password if prompted. |
| **Example:** Router> enable |
| **Step 2** configure terminal | Enters global configuration mode. |
| **Example:** Router# configure terminal |
| **Step 3** ip dhcp pool pool-name | Creates a name for the DHCP server address pool and enters DHCP pool configuration mode. |
| **Example:** Router(config)# ip dhcp pool pool2 |
| **Step 4** host ip-address subnet-mask | Specifies the IP address that you want the phone to get. |
| **Example:** Router(config-dhcp)# host 10.0.0.0 255.255.0.0 |
| **Step 5** client-identifier mac-address | Specifies the MAC address of the phone, which is printed on a sticker on each Cisco Unified IP phone.  
**Note:** You must use a 01 prefix number before the MAC address. |
| **Example:** Router(config-dhcp)# client-identifier 01238.380.3056 |
| **Step 6** option 150 ip ip-address | Specifies the TFTP server IP address from which the Cisco Unified IP phone downloads the image configuration file, XmlDefault.cnf.xml. This is your Cisco Unified CME router IP address. |
| **Example:** Router(config-dhcp)# option 150 ip 10.0.0.1 |
| **Step 7** default-router ip-address | (Optional) Specifies the router that the IP phones will use to send or receive IP traffic that is external to their local subnet. |
| **Example:** Router(config-dhcp)# default-router 10.0.0.1 |

If the Cisco Unified CME router is the only router on the network, this address should be the Cisco Unified CME IP source address. This command can be omitted if IP phones need to send or receive IP traffic only to or from devices on their local subnet.

The IP address that you specify for default router will be used by the IP phones for fallback (Survivable Remote Site Telephony or SRST) purposes. If the Cisco Unified CME IP source address becomes unreachable, IP phones will attempt to register to the address specified in this command.
## Defining a DHCP Relay Server

The Cisco IOS DHCP relay server feature is enabled on routers by default. If the DHCP relay server becomes disabled for some reason and you need it, use the steps in this task to enable it.

This task sets up DHCP relay on the LAN interface where the Cisco Unified IP phones are connected and enables the Cisco IOS DHCP server feature to relay requests from DHCP clients (phones) to a DHCP server.

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `service dhcp`
4. `interface type number`
5. `ip helper-address ip-address`

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> <code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router&gt; enable</code></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> <code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> <code>service dhcp</code></td>
<td>Enables the Cisco IOS DHCP server feature on the router.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router(config)# service dhcp</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> <code>interface type number</code></td>
<td>Enters interface configuration mode for the specified interface.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router(config)# interface vlan 10</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> <code>ip helper-address ip-address</code></td>
<td>Specifies the helper address for any unrecognized broadcast for TFTP server and DNS server requests. Each server requires a separate <code>ip helper-address</code> command if the servers are on different hosts. You can also configure multiple TFTP server targets by using the <code>ip helper-address</code> commands for multiple servers.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router(config-if)# ip helper-address 10.0.0.1</code></td>
<td></td>
</tr>
</tbody>
</table>
Changing the TFTP Server Address

When phones need the address of the TFTP server from which they will download phone firmware and configuration files, they get it from the DHCP server. If you need to change the TFTP server address after it has been configured, you must also change the TFTP IP address on the DHCP server and reset the phones so that they recontact the DHCP server for the new TFTP address.

**Step 1**
Use one of the following steps to change the TFTP server address on the DHCP server:

- If the DHCP server is on the Cisco Unified CME router, modify the DHCP pool using the `option 150 ip` command to change the TFTP IP address.
- If the DHCP server is on a different router than Cisco Unified CME, reconfigure the external DHCP server with the new IP address of the TFTP server.

**Step 2**
Reset all phones using the `reset` command.

Setting Network Time Protocol

Network Time Protocol (NTP) allows you to synchronize your Cisco Unified CME router to a single clock on the network, which is known as the clock master. NTP is disabled on all interfaces by default, but it is essential for Cisco Unified CME so you must ensure that it is enabled. For more information, see the “Performing Basic System Management” chapter of the Cisco IOS Network Management Configuration Guide.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `clock timezone zone hours-offset [minutes-offset]`
4. `clock summer-time zone recurring [week day month hh:mm week day month hh:mm [offset]]`
5. `ntp server ip-address`
6. `create cnf-files`
7. `restart {all [time-interval] | mac-address}`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router&gt; enable</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router# configure terminal</code></td>
<td></td>
</tr>
</tbody>
</table>
### Command or Action

<table>
<thead>
<tr>
<th>Step 3</th>
<th>clock timezone zone hours-offset [minutes-offset]</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config)# clock timezone pst -8</td>
</tr>
</tbody>
</table>

### Purpose
- Sets the local time zone.
- **zone**—Name of the time zone (typically a standard abbreviation).
- **hours-offset**—Number of hours that the specified time zone differs from Coordinated Universal Time (UTC).
- **minutes-offset**—(Optional) Number of minutes that the time zone differs from UTC.

| Step 4 | clock summer-time zone recurring [week day month hh:mm | week day month hh:mm [offset]] |
|--------|---------------------------------------------------------|
| **Example:** | Router(config)# clock summer-time pdt recurring |

### Purpose
- (Optional) Specifies daylight savings time.
- **zone**—Name of the time zone (typically a standard abbreviation).

Default is that summer time is disabled. If the **clock summer-time zone recurring** command is specified without parameters, the summer time rules default to United States rules. Default of the **offset** argument is 60.

For more information, refer to the “Performing Basic System Management” chapter of *Cisco IOS Network Management Configuration Guide*.

<table>
<thead>
<tr>
<th>Step 5</th>
<th>ntp server ip-address</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config)# ntp server 10.1.2.3</td>
</tr>
</tbody>
</table>

### Purpose
- Allows the clock on this router to be synchronized with the specified NTP server.
- **ip-address**—IP address of the time server that provides the clock synchronization.

<table>
<thead>
<tr>
<th>Step 1</th>
<th>telephony-service</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config)# telephony-service</td>
</tr>
</tbody>
</table>

### Purpose
- Enters telephony-service configuration mode.

<table>
<thead>
<tr>
<th>Step 2</th>
<th>create cnf-files</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-telephony)# create cnf-files</td>
</tr>
</tbody>
</table>

### Purpose

| Step 3 | restart {all [time-interval] | mac-address} |
|--------|-----------------------------------------------|
| **Example:** | Router(config-telephony)# restart all |

### Purpose
- Performs a fast reboot of the specified phone or all phones associated with this Cisco Unified CME router. Does not contact the DHCP or TFTP server for updated information.
- **all**—Restarts all phones associated with a Cisco Unified CME router.
- **time-interval**—(Optional) Time interval, in seconds, between the beginning of each phone restart. Range is from 0 to 60. Default is 15.
- **mac-address**—Restarts the phone that has the specified MAC address.
Examples

The following example defines the pst timezone as 8 hours offset from UTC, using a recurring daylight savings time called pdt, and synchronizes the clock with the NTP server at 10.1.2.3.

clock timezone pst -8
clock summer-time pdt recurring
ntp server 10.1.2.3

Configuring DTMF Relay for H.323 Networks

Note

This procedure is required only when you are setting up multi-site installations.

IP phones connected to Cisco Unified CME systems require the use of out-of-band DTMF relay to transport DTMF (keypad) digits across VoIP connections. The reason for this is that the codecs used for in-band transport may distort DTMF tones and make them unrecognizable. DTMF relay solves the problem of DTMF tone distortion by transporting DTMF tones out-of-band, or separate, from the encoded voice stream.

For IP phones on H.323 networks, DTMF is relayed using the H.245 alphanumeric method, which is defined by the ITU H.245 standard. This method separates DTMF digits from the voice stream and sends them as ASCII characters in H.245 user input indication messages through the H.245 signaling channel instead of the RTP channel. For more information, refer to the “Configuring H.323 Gateways” chapter of the Cisco IOS H.323 Configuration Guide.

Note

For DTMF relay on SIP networks, refer to the configuration instructions in the “SIP Trunk Features” section on page 275.

SUMMARY STEPS

1. dial-peer voice tag voip
2. dtmf-relay h245-alphanumeric
3. exit

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enters dial-peer configuration mode.</td>
</tr>
<tr>
<td>dial-peer voice tag voip</td>
<td></td>
</tr>
</tbody>
</table>
Task 5: Setting Cisco Unified CME Parameters

The commands in this task identify and modify eXtensible Markup Language (XML) phone configuration files so that IP phones can automatically find the defaults to configure themselves when they come online or are rebooted. The last step in this task is to reset all phones, which causes them to request new configuration files.

When auto-registration is enabled (the default), the Cisco Unified CME system assigns an ephone slot to any ephone that is connected to the system, whether the ephone has been explicitly configured or not. You can disable this capability using the no auto-reg-ephone command to prevent unauthorized phones from connecting to the system.

The following topics are discussed in this section:

- Special Note About the transfer-system Command, page 61
- Special Parameters for Cisco Unified IP Phone 7970G and 7971G-GE, page 62
- Configuring Cisco Unified CME Parameters, page 62

Note

If you are using the Cisco IPC Express Quick Configuration Tool (QCT), this task is performed automatically by the tool. Proceed to the “Task 7: Plugging in Phones” section on page 76.
Special Note About the transfer-system Command

The `transfer-system` command specifies whether the H.450.2 standard or a Cisco proprietary method is used to communicate call-transfer information across the network.

Prior to Cisco Unified CME 4.0, the default for this command specified the Cisco proprietary method. In Cisco Unified CME 4.0, the default was changed to the H.450.2 standard. Table 16 contains configuration recommendations for different Cisco Unified CME versions. Also see the “Transfer and Forwarding Support” section on page 223 for more information about call-transfer methods.

When you specify use of the H.450.2 consultative or blind mode of transfer globally by using the `transfer-system` command (or by using the default), you can override that mode for individual phones by using the `transfer-mode` command.

<table>
<thead>
<tr>
<th>Cisco Unified CME Version</th>
<th>transfer-system Command Default</th>
<th>transfer-system Keyword Recommendation</th>
<th>Explanation of Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.0 and later versions</td>
<td><code>full-consult</code></td>
<td><code>full-consult</code> or <code>full-blind</code></td>
<td>Use H.450.2 for call transfer, which is the default for this version. You do not need to use the <code>transfer-system</code> command unless you want to use the <code>full-blind</code> or <code>dss</code> keyword. Optionally, you can use the proprietary Cisco method by using the <code>transfer-system</code> command with the <code>blind</code> or <code>local-consult</code> keyword.</td>
</tr>
<tr>
<td>3.0 to 3.3</td>
<td><code>blind</code></td>
<td><code>full-consult</code> or <code>full-blind</code></td>
<td>Use H.450.2 for call transfer. You must explicitly configure the <code>transfer-system</code> command with the <code>full-consult</code> or <code>full-blind</code> keyword because H.450.2 is not the default for these versions. Optionally, you can use the proprietary Cisco method by using the <code>transfer-system</code> command with the <code>blind</code> or <code>local-consult</code> keyword.</td>
</tr>
<tr>
<td>2.1 to 3.0</td>
<td><code>blind</code></td>
<td><code>blind</code> or <code>local-consult</code></td>
<td>Use the Cisco proprietary method, which is the default for this version. You do not need to use the <code>transfer-system</code> command unless you want to use the <code>local-consult</code> keyword. Optionally, you can use H.450.2 for call transfer by using <code>transfer-system</code> command with the <code>full-consult</code> or <code>full-blind</code> keyword. You must also configure the router with a Tcl script that is contained in the file called app-h450-transfer.x.x.x.x.zip. This file is posted on the Cisco Unified CME software download website at <a href="http://www.cisco.com/cgi-bin/tablebuild.pl/ip-iostsp">http://www.cisco.com/cgi-bin/tablebuild.pl/ip-iostsp</a>. For configuration information, see the Cisco IOS Telephony Services V2.1 guide.</td>
</tr>
<tr>
<td>Earlier than 2.1</td>
<td><code>blind</code></td>
<td><code>blind</code></td>
<td>Use the Cisco proprietary method, which is the default for this version. You do not need to use the <code>transfer-system</code> command unless you want to use the <code>local-consult</code> keyword.</td>
</tr>
</tbody>
</table>
Special Parameters for Cisco Unified IP Phone 7970G and 7971G-GE

The clocks in the Cisco Unified IP Phone 7970G and 7971G-GE units obtain Coordinated Universal Time (UTC) from their Cisco Unified CME router’s clocks. To display the correct local time, the time for most Cisco Unified IP Phone 7970G and 7971G-GE units must be offset using the `time-zone` command.

The `service phone` command sets display and functionality parameters for Cisco Unified IP Phone 7970G and 7971G-GE units in a Cisco Unified CME system. The command works with the vendorConfig section of the SEP*.conf.xml configuration file, which is read by the phone firmware when a Cisco Unified IP Phone 7970G or 7971G-GE is booted. The following text shows the format of an entry created in a SEP*.conf.xml file:

```
<vendorConfig>
  <parameter-name>parameter-value</parameter-name>
</vendorConfig>
```

Only the vendorConfig parameters that are supported by the currently loaded firmware are available. The number and type of parameters may vary from one Cisco Unified IP Phone 7970G or 7971G-GE firmware version to the next.

For changes to the time-zone and service-phone settings to take effect, the SEP*.conf.xml file must be updated using the `create cnf-files` command and the Cisco Unified IP Phone 7970G or 7971G-GE units must be rebooted using the `reset` command.

The `show telephony-service tftp-binding` command allows you to view the SEP*.cnf.xml files that are associated with individual phones.

Restrictions

The following phones only support the United States language code. For these phones, the `user-locale` and `network-locale` commands must be set to their default, United States (US).

- Cisco Unified IP Phone 7910
- Cisco Unified IP Phone Expansion Module 7914
- Cisco Unified IP Conference Station 7935
- Cisco Unified IP Conference Station 7936
- Cisco Unified IP Phone 7970G
- Cisco Unified IP Phone 7971G-GE

Configuring Cisco Unified CME Parameters

This task sets values for the telephony parameters that the Cisco Unified CME system requires, rebuilds the phone configuration files, and resets the phones so that they download new parameter values.

SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `tftp-server flash:filename`
4. `telephony-service`
1. **max-ephones max-phones**
2. **max-dn max-directory-numbers** [**preference** preference-order] [**no-reg** primary | **both**]
3. **auto-reg-ephone**
4. **load** phone-type firmware-file
5. **ip source-address** ip-address [**port** port] [any-match | strict-match]
6. **user-locale language-code**
7. **network-locale locale-code**
8. **date-format** [mm-dd-yy | dd-mm-yy | yy-dd-mm | yy-mm-dd]
9. **time-format** {12 | 24}
10. **time-zone** number
11. **service phone** parameter-name parameter-value
12. **create cnf-files**
13. **keepalive seconds**
14. **transfer-system** {blind | full-blind | full-consult [dss] | local-consult}
15. **reset all** [**time-interval**]
16. **exit**

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>
### Command or Action | Purpose
--- | ---
**Step 3** tftp-server flash:filename | Permits the Cisco Unified CME router to provide TFTP access to the specified file by the IP phones served by the router. Repeat this command for each phone firmware file needed for phones at your site. You may have already used this command in Step 3 of Task 3: Downloading Cisco Unified CME Software. If you have not used this command yet, you must use it now for each phone firmware file you require at your site.

**Example:**
Router(config)# tftp-server flash:P00307020300.bin

**Note** The phone version is derived from the final eight digits of the phone firmware filename. For example, [P00307020300] is phone version 7.2(3.0).

**Step 4** telephony-service | Enters telephony-service configuration mode.

**Example:**
Router(config)# telephony-service

**Step 5** max-ephones max-phones | Sets the maximum number of Cisco Unified IP phones to be supported by this router. The maximum number of phones is platform- and version-dependent. Refer to CLI help.

**Example:**
Router(config-telephony)# max-ephones 24

**Step 6** max-dn max-directory-numbers [preference preference-order] [no-reg primary | both] | Sets the maximum number of extensions (ephone-dns) that can exist in a Cisco Unified CME system.

- max-directory-numbers—The maximum number of ephone-dns that can be defined for this system. The range is platform- and version-dependent. Refer to CLI help for this information.

- preference preference-order—(Optional) Sets a preference value for the primary number of an ephone-dn. Refer to CLI help for a range of numeric options, where 0 is the highest preference. Default is 0.

- no-reg—(Optional) Globally disables all ephone-dn registration to an H.323 gatekeeper or SIP proxy.

- primary—Primary ephone-dn numbers only.

- both—Primary and secondary ephone-dn numbers.

**Note** You can disable registration for individual ephone-dns by using the number command.
### Step 7: Setting Cisco Unified CME Parameters

**Example:**

```sh
Router(config-telephony)# no auto-reg-ephone
```

(Optional) Enables automatic registration of all ephones that attempt to register. This is the default.

The `no` form of this command blocks the automatic registration of ephones that do not have their MAC addresses explicitly listed in the configuration. When automatic registration is disabled, the system keeps a log of phones that attempt to register but that are denied. The log contains the date and time of the attempt, the type of phone, and the MAC address.

The `show ephone attempted-registrations` command displays a log of the denied attempts to register. The `clear telephony-service ephone-attempted-registrations` command empties the log.

See the example in the “Blocking Automatic Registration: Example” section on page 69.

### Step 8: load phone-type firmware-file

**Example:**

```sh
Router(config-telephony)# load 7960-7940 P00307020300
```

Identifies a Cisco Unified IP phone firmware file to be used by phones of the specified Cisco Unified IP phone type when they register. Repeat this command for each firmware file you need at your site.

- **phone-type**—Type of IP phone. Consult CLI help for valid entries.
- **firmware-file**—Filename of the phone firmware, without the filename suffix.

**Note** If a firmware file that you are loading for a particular phone type is larger than 384KB, you must first load a file on that phone type that is smaller than 384KB, then load the larger file.

### Step 9: ip source-address ip-address [port port] [any-match | strict-match]

**Example:**

```sh
Router(config-telephony)# ip source-address 10.16.32.144
```

Identifies the IP address and port number that the Cisco Unified CME router uses for IP phone registration. The default port is 2000.

- **any-match**—(Optional) Disables strict IP address checking for registration. This is the default.
- **strict-match**—(Optional) Instructs the router to reject IP phone registration attempts if the IP server address used by the phone does not exactly match the source address.

### Step 10: user-locale language-code

**Example:**

```sh
Router(config-telephony)# user-locale FR
```

(Optional; see the “Restrictions” section on page 62) Specifies a language for display on the Cisco Unified IP Phones 7940 and 7940G and Cisco Unified IP Phones 7960 and 7960G.

- **language-code**—Refer to CLI help for a list of ISO-3166 codes that are supported. United States (US) is the default.
### Command or Action

**Step 11**

network-locale  locale-code  

*Example:*

Router(config-telephony)# network-locale FR

(Optional: see the “Restrictions” section on page 62) Specifies a set of call progress tones and cadences on the Cisco Unified IP Phones 7940 and 7940G and Cisco Unified IP Phones 7960 and 7960G.

- `locale-code`—Refer to CLI help for a list of ISO-3166 codes that are supported. United States (US) is the default.

**Step 12**

date-format {mm-dd-yy | dd-mm-yy | yy-dd-mm | yy-mm-dd}  

*Example:*

Router(config-telephony)# date-format yy-dd-mm

(Optional) Sets the date format for IP phone display. The choices are `mm-dd-yy`, `dd-mm-yy`, `yy-dd-mm`, and `yy-mm-dd`, where:

- `dd`—day
- `mm`—month
- `yy`—year
- Default is `mm-dd-yy`.

**Step 13**

time-format {12 | 24}  

*Example:*

Router(config-telephony)# time-format 24

(Optional) Selects a 12-hour clock or 24-hour clock for the time display format on all Cisco Unified IP phones attached to the router.

- Default is `12`.

**Step 14**

time-zone number  

*Example:*

Router(config-telephony)# time-zone 2

(Optional: Cisco Unified IP Phone 7970G and 7971G-GE only) Sets time zone.

- `number`—Numeric time zone name. Refer to CLI help or the Cisco Unified CallManager Express Command Reference for a list of the time-zone numbers. The default is time zone 5, Pacific Standard/Daylight Time (-480).

**Step 15**

service phone  parameter-name  parameter-value  

*Example:*

Router(config-telephony)# service phone garp 0

(Optional: Cisco Unified IP Phone 7970G and 7971G-GE only) Sets display and phone functionality using the vendorConfig parameters from the Sep*.conf.xml configuration file.

- See the Cisco Unified CallManager Express Command Reference for a complete description of this command.

**Step 16**

create cnf-files  

*Example:*

Router(config-telephony)# create cnf-files

Builds the XML configuration files that are required for Cisco Unified CME phones.

**Step 17**

keepalive  seconds  

*Example:*

Router(config-telephony)# keepalive 45

(Optional) Sets the time interval, in seconds, between keepalive messages that are sent to the router by Cisco Unified IP phones. The default is usually adequate. If the interval is set too large, it is possible that notification will be delayed when a system goes down.

- `seconds`—Range is from 10 to 65535. Default is 30.
### Command or Action

**Step 18**

```
transfer-system {blind | full-blind | full-consult [dss] | local-consult}
```

**Example:**

```
Router(config-telephony)# transfer-system
full-consult
```

### Purpose

Specifies call transfer method.

- **For H.323 networks and Cisco CME 3.0 or later,** specify H.450.2 call transfers using the `full-blind` or `full-consult` keyword. For Cisco CME versions from 3.0 to 3.3, you must explicitly configure the `full-consult` or `full-blind` keyword to use H.450.2 standards.

- **For H.323 networks and Cisco ITS 2.1 and earlier versions,** use the `local-consult` or `blind` keyword to specify a Cisco proprietary call transfer method. (Cisco ITS 2.1 can specify H.450.2 transfer by using the `full-blind` or `full-consult` keyword and the Tcl script in the file called app-h450-transfer.x.x.x.x.zip.)

- **For SIP networks,** use only the `full-blind` or `full-consult` keyword. For more information about SIP, refer to “SIP Trunk Features” section on page 275 in this guide and to the *Cisco IOS SIP Configuration Guide*.

**Note**

For Cisco Unified CME 4.0 and later versions, the default is the `full-consult` keyword. For earlier versions, the default is the `blind` keyword.

- **blind**—Calls are transferred without consultation with a single phone line using the Cisco-proprietary method. For Cisco CME versions earlier than 4.0, this is the default.

- **full-blind**—Calls are transferred without consultation using H.450.2 standard methods.

- **full-consult**—Calls are transferred with consultation using H.450.2 standard methods and a second phone line if available. The calls fall back to full-blind if the second line is unavailable. For Cisco Unified CME 4.0 and later versions, this is the default.

- **dss**—Calls are transferred with consultation to idle monitor lines. All other call-transfer behavior is identical to full-consult.

- **local-consult**—Calls are transferred with local consultation using a second phone line if available. The calls fall back to blind for nonlocal consultation or nonlocal transfer target.
Verifying Cisco Unified CME Parameters

### Step 1
Use the `show running-config` command to verify the settings you made.

### Examples

This section contains the following examples:
- Basic Cisco Unified CME Parameters: Example
- Blocking Automatic Registration: Example
Basic Cisco Unified CME Parameters: Example

The following example defines a Cisco Unified CME system with 100 ephones and 500 ephone-dns. It sets up TFTP file sharing for phone firmware files for Cisco Unified IP Phone 7905, 7912, 7914, 7920, 7940, 7960, and 7970 phone types and loads those files.

```
! tftp-server flash:CP7905040000SCCP040701A.sbin
  tftp-server flash:CP7912040000SCCP040701A.sbin
  tftp-server flash:TERM70.7-0-1-18S.LOADS
  tftp-server flash:S00104000100.sbn
  tftp-server flash:P00307020300.bin
  tftp-server flash:P00307020300.loads
  tftp-server flash:P00307020300.sb2
!
  telephony-service
    max-ephones 100
    max-dn 500
    load 7960-7940 P00307020300
    load 7914 S00104000100
    load 7905 CP7905040000SCCP040701A
    load 7920 cmterm_7920.4.0-02-00
    load 7970 TERM70.7-0-1-18S
    load 7912 CP7912040000SCCP040701A
    ip source-address 10.16.32.144 port 2000
    create cnf-files version-stamp Jan 01 2002 00:00:00
    keepalive 45
    transfer-system full-consult
.
.
.
Blocking Automatic Registration: Example

The following example disables automatic ephone registration, displays the log of attempted registrations, and then clears the log.

```
Router(config)# telephony-service
Router(config-telephony)# no auto-reg-ephone
Router(config-telephony)# exit
Router(config)# exit
Router# show ephone attempted-registrations

Attempting Mac address:

<table>
<thead>
<tr>
<th>Num</th>
<th>Mac Address</th>
<th>DateTime</th>
<th>DeviceType</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>C863.8475.5417</td>
<td>22:52:05 UTC Thu Apr 28 2005</td>
<td>SCCP Gateway (AN)</td>
</tr>
<tr>
<td>2</td>
<td>C863.8475.5408</td>
<td>22:52:05 UTC Thu Apr 28 2005</td>
<td>SCCP Gateway (AN)</td>
</tr>
<tr>
<td>25</td>
<td>000D.28D7.7222</td>
<td>22:26:32 UTC Thu Apr 28 2005</td>
<td>Telecaster 7960</td>
</tr>
<tr>
<td>26</td>
<td>000D.BD87.A9EA</td>
<td>22:25:59 UTC Thu Apr 28 2005</td>
<td>Telecaster 7960</td>
</tr>
<tr>
<td>47</td>
<td>C863.94A8.D40F</td>
<td>22:52:17 UTC Thu Apr 28 2005</td>
<td>SCCP Gateway (AN)</td>
</tr>
<tr>
<td>49</td>
<td>C863.94A8.D400</td>
<td>22:52:15 UTC Thu Apr 28 2005</td>
<td>SCCP Gateway (AN)</td>
</tr>
</tbody>
</table>

Router# clear telephony-service ephone-attempted-registrations
Troubleshooting Tips

- To determine the recommended phone firmware filenames for each phone type and Cisco Unified CME version, see the Cisco CallManager Express Supported Firmware, Platforms, Memory, and Voice Products for that version. The link to this document for your Cisco Unified CME version can be found in the Cisco Unified CME Documentation Roadmap.
- Use the `debug ephone register` command to show status (alarm) messages at registration time. The messages include the current IP phone firmware version.
- To display the current locale codes that are associated with dictionary, language, and call progress tone files, use the `show telephony-service tftp-bindings` command.
- Use the `debug ephone sccp-state` command to output only the debug messages that correspond to the SCCP messages that are sent to IP phones to indicate the SCCP phone call state.

Related Features

Externally Stored and Per-Phone Configuration Files
Cisco Unified CME 4.0 and later versions provide the ability to store large configuration files on external TFTP servers and to provide individualized configuration files for each phone or phone type. For more information, see the “Externally Stored and Per-Phone Configuration Files” section on page 93.

Alternative and User-Defined User and Network Locales
Cisco Unified CME 4.0 and later versions let you name up to five user and network locales for phones in your Cisco Unified CME system to use. You can also download files to add new user and network locales. For more information, see the “Alternative User and Network Locales” section on page 97 and the “User-Defined User and Network Locales” section on page 105.

Call Hunt (Preference)
The `max-dn` command allows you to specify a preference value for the primary number of all ephone-dns that are created. For more information about ephone-dn dial-peer preference, see the “Call Hunt” section on page 379.

Redundant Router
You can set up a secondary Cisco Unified CME router to serve as a backup if the primary router fails. For more information, see the “Redundant Router” section on page 351.

Task 6: Provisioning Phones

This task sets up the initial ephone-dn-to-ephone relationships—that is, what extensions appear in what order on what phones. When you have completed this task, you will be able to make and receive basic calls.

For more information about ephones and the different types of ephone-dns, see the “Basic Cisco Unified CME Concepts” section on page 24 in the “Cisco Unified CallManager Express Overview” chapter.

In this process you set up individual ephone-dns and then associate each with a button or buttons on one or more ephones.
Each ephone-dn becomes a virtual line, or extension, on which call connections can be made. Each ephone-dn automatically creates one or more virtual dial peers and virtual voice ports to make those call connections.

Each physical phone in your system must be configured as an ephone on the Cisco Unified CME router to receive support in the LAN environment.

Using the `ephone-dn` command and the `dual-line` keyword, you can create an ephone-dn in dual-line mode. Each dual-line ephone-dn has one voice port and two channels to handle two independent calls. This mode enables call waiting, call transfer, and conference functions on a single ephone-dn. Dual-line mode works with all phone types, but is not appropriate for ephone-dns that are used for voice-mail numbers, intercoms, message-waiting indicators, paging, or hunt groups. Overlays and hunt groups that use dual-line ephone-dns are supported. Only one dual-line ephone-dn can be set on a Cisco Unified IP Phone 7910.

The `button` command in ephone configuration mode allows you to customize ring characteristics for each button or to designate buttons that should not produce an audible ring when they receive incoming calls. The feature-ring and silent-ring features are supported on all phones but are most appropriate for multiline IP phones, including the Cisco Unified IP Phones 7940 and 7940G, Cisco Unified IP Phones 7960 and 7960G, and Cisco Unified IP Phone Expansion Module 7914.

If you are using the Cisco IPC Express Quick Configuration Tool (QCT), this task is performed automatically by the tool. Proceed to the “Task 7: Plugging in Phones” section on page 76.

### Prerequisites

- Cisco IOS software and Cisco Unified CME software must be installed in router flash memory.
- The steps described in the “Task 4: Defining Network Settings” section on page 52 and the “Task 5: Setting Cisco Unified CME Parameters” section on page 60 must be completed before you start the task described in this section.

### Provisioning Phones Using Cisco IOS Software CLI

This task uses Cisco IOS software to provision phones.

If you are using the QCT to provision phones, see *Installing Cisco IPC Express: Cisco CallManager Express and Cisco Unity Express*.

#### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `ephone-dn dn-tag [dual-line]`
4. `number number [secondary number] [no-reg [both | primary]]`
5. `name name`
6. `exit`
7. `ephone phone-tag`
8. `mac-address [mac-address]`
9. `type phone-type [addon 1 module-type [2 module-type]]`

10. `button button-number{separator}dn-tag [,dn-tag...] [button-number{x}overlay-button-number] [button-number...]`

11. keepalive seconds

12. keypad-normalize

13. Proceed to the “Task 7: Plugging in Phones” section on page 76.

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> ephone-dn dn-tag [dual-line]</td>
<td>Enters ephone-dn configuration mode, creates an ephone-dn, and optionally assigns it dual-line status.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router(config)# ephone-dn 55 dual-line</code></td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong> To change an ephone-dn from dual-line to single-line mode or the reverse, you must first delete the ephone-dn and then recreate it.</td>
<td></td>
</tr>
</tbody>
</table>

| **Step 2** number number [secondary number] [no-reg [both | primary]] | Configures a valid extension number for this ephone-dn instance. |
| **Example:** | |
| `Router(config-ephone-dn)# number 2345` | |
| **Profile** | |
| number—String of up to 16 digits that represents a telephone or extension number to be associated with this ephone-dn. |
| secondary—(Optional) Allows you to associate a second telephone number with an ephone-dn. |
| no-reg—(Optional) Specifies that this number should not register with the H.323 gatekeeper. Unless you specify one of the optional keywords (both or primary) after the no-reg keyword, only the secondary number is not registered. |

| **Step 3** name name | (Optional) Associates a name with this ephone-dn instance. This name is used for caller-ID displays and in the local directory listings. |
| **Example:** | |
| `Router(config-ephone-dn)# name Smith, John` | |
| You must follow the name order that is specified in the directory command in telephony-service configuration mode (either first-name-first or last-name-first). |
### Command or Action

<table>
<thead>
<tr>
<th>Step 4</th>
<th><strong>exit</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td><code>Router(config-ephone-dn)# exit</code></td>
</tr>
<tr>
<td><strong>Purpose:</strong></td>
<td>Exits ephone-dn configuration mode.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 5</th>
<th><strong>ephone phone-tag</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td><code>Router(config)# ephone 6</code></td>
</tr>
<tr>
<td><strong>Purpose:</strong></td>
<td>Enters ephone configuration mode.</td>
</tr>
<tr>
<td>-</td>
<td><code>phone-tag</code>—Unique sequence number that identifies this ephone during configuration tasks. The maximum number of ephones for a particular Cisco Unified CME system is version- and platform-specific. For the range of values, refer to CLI help.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 6</th>
<th><strong>mac-address</strong> [mac-address]</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td><code>Router(config-ephone)# mac-address 2946.3f2.311</code></td>
</tr>
<tr>
<td><strong>Purpose:</strong></td>
<td>Specifies the MAC address of the IP phone that is being configured.</td>
</tr>
<tr>
<td>-</td>
<td><code>mac-address</code>—(Optional) MAC address on the bottom of an IP phone. If you choose to register phones before configuring them, the <strong>mac-address</strong> command can be used during configuration without entering the <strong>mac-address</strong> argument. The Cisco Unified CME system detects MAC addresses and automatically populates phone configurations with their corresponding MAC addresses and phone types. This capability is supported only for Cisco Unified CME 3.0 and later versions, and is not supported for voice-mail ports.</td>
</tr>
</tbody>
</table>
Step 7

```
type phone-type [addon 1 module-type
2 module-type]
```

**Example:**
```
Router(config-ephone)# type 7960 addon 1 7914
```

( Optional) Specifies the type of phone. This command is required for phones with ATA devices and when you enter an add-on module. For other phone types, this command is optional.

**Note**
For Cisco Unified CME 4.0 and later versions, the only types to which you can apply an add-on module are 7960, 7961, 7961GE, and 7970. For Cisco CME 3.4 and earlier versions, the only type to which you can apply an add-on module is 7960.

- **phone-type**—Valid entries are the following:
  - 7902—Cisco Unified IP Phone 7902G.
  - 7905—Cisco Unified IP Phone 7905G.
  - 7910—Cisco Unified IP Phone 7910 and 7910G.
  - 7911—Cisco Unified IP Phone 7911G.
  - 7912—Cisco Unified IP Phone 7912G.
  - 7920—Cisco Unified Wireless IP Phone 7920.
  - 7935—Cisco Unified IP Conference Station 7935.
  - 7936—Cisco Unified IP Conference Station 7936.
  - 7940—Cisco Unified IP Phones 7940 and 7940G.
  - 7941—Cisco Unified IP Phone 7941G.
  - 7941GE—Cisco Unified IP Phone 7941G-GE.
  - 7960—Cisco Unified IP Phones 7960 and 7960G.
  - 7961—Cisco Unified IP Phones 7940 and 7961G.
  - 7961GE—Cisco Unified IP Phone 7961GE.
  - 7970—Cisco Unified IP Phone 7970G.
  - 7971—Cisco Unified IP Phone 7971G-GE.
  - anl—Analog.
  - ata—Cisco ATA-186 or Cisco ATA-188.
  - CIPC—Cisco IP Communicator.

- **module-type**—Valid entry is the following:
  - 7914—Cisco Unified IP Phone 7914 Expansion Module.
### Step 8

**Command or Action**

```plaintext
button button-number{separator}dn-tag
[,...dn-tag...]
[button-number(x)overlay-button-number]
[button-number...]
```

**Purpose**

Associates a button number and line characteristics with an extension (ephone-dn). Maximum number of buttons is determined by phone type.

**Note**

The Cisco Unified IP Phone 7910 has only one line button, but can be given two ephone-dn tags.

- **button-number**—Number of a line button on an IP phone, starting with 1 as the top button.
- **separator**—Single character that denotes the type of characteristics to be associated with the button.
  - : (colon)—Normal ring.
  - b—Beep for call waiting is allowed.
  - c—Call waiting is allowed on an overlaid ephone-dn.
  - f—Feature ring. Triple-pulse cadence.
  - m—Monitor mode for a shared line.
  - o—Overlaid line. Up to 25 ephone-dns share a single button. The `dn-tag` argument can contain up to 25 dn-tags, separated by commas.
  - s—Silent ring. Audible ring and call-waiting beep are suppressed for incoming calls.
- **dn-tag**—Unique sequence number of the ephone-dn that you want to appear on this button. For overlay lines (separator is o or c), this argument can contain up to 25 ephone-dn tags, separated by commas.
- **x**—Separator that creates an overlay rollover button.
- **overlay-button-number**—Number of the overlay button that should overflow to this button.

**Example:**

```plaintext
Router(config-ephone)# button 1:10 2:11 3b12 4o13,14,15
```

### Step 9

**Command or Action**

`keepalive seconds`

**Purpose**

(Optional) Sets the length of the time interval between successive keepalive messages from the Cisco CallManager Express router to a particular IP phone.

- **seconds**—Interval time, in seconds. Range is from 10 to 65535. Default is 30.

**Example:**

```plaintext
Router(config-ephone)# keepalive 200
```

### Step 10

**Command or Action**

`keypad-normalize`

**Purpose**

(Optional) Imposes a 200-millisecond delay before each keypad message from an IP phone.

**Example:**

```plaintext
Router(config-ephone)# keypad-normalize
```

### Step 11

Proceed to the “Task 7: Plugging in Phones” section on page 76.
Task 7: Plugging in Phones

After provisioning phones, you can start plugging them in. Each phone will register with Cisco Unified CME and download its phone firmware and configuration file when it is first plugged in. If you prevent auto-registration by using the `no auto-reg-ephone` command in Task 5: Setting Cisco Unified CME Parameters, the only phones that will be able to register are the phones whose MAC addresses you specified in Task 6: Provisioning Phones.

Task 8: Resetting and Restarting Phones

Cisco Unified IP phones must be rebooted after configuration changes in order for the changes to take effect. There are two ways to reboot a phone: using the `reset` command and using the `restart` command. The differences between these commands are summarized in Table 17.

Examples

The following example assigns extension 2225 in the Accounting Department to button 1 on ephone 2.

```
ephone-dn 25
  number 2225
  name Accounting

ephone 2
  mac-address 00E1.CB13.0395
  type 7960
  button 1:25
```

Related Features

**Ephone-dn Templates**
Some basic ephone-dn features, such as description, can be set using ephone-dn templates. For more information, see the “Ephone-dn Templates” section on page 322.

**Ephone Templates**
Some basic phone features, such as type and keepalive interval, can be set using ephone templates. For more information, see the “Ephone Templates” section on page 318.
Task 8: Resetting and Restarting Phones

With either of these commands, you can reboot a single phone or you can reboot all phones in a Cisco Unified CME system. When you use the `reset` command to reboot multiple IP phones, it is possible for a conflict to occur if too many phones attempt to access changed Cisco Unified CME configuration information via TFTP simultaneously. The `sequence-all` keyword has been provided to specify a sequential reset of multiple IP phones to minimize the risk of that conflict.

The `reset` command takes significantly longer to process than the `restart` command when you are updating multiple phones, but it must be used when you update phone firmware, user locale, network locale, or URL parameters. For simple button, line, or speed-dial changes, use the `restart` command.

This section describes the following tasks:

- Using the `reset` Command, page 77
- Using the `restart` Command, page 79

### Using the `reset` Command

The `reset` command must be used to reboot IP phones after you update phone firmware, user locale, network locale, or URL parameters. A phone reset takes longer than a phone restart because the DHCP and TFTP servers are contacted for updates. You can reset one phone or all phones from telephony-service configuration mode, or you can reset a single phone from ephone configuration mode.

#### SUMMARY STEPS

1. `enable`
2. `configure terminal`
1. `telephony-service`
2. `reset {all [time-interval] | cancel | mac-address mac-address | sequence-all}`

#### Table 17  `reset` and `restart` Command Differences

<table>
<thead>
<tr>
<th></th>
<th><code>reset</code> Command</th>
<th><code>restart</code> Command</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Type of Reboot</strong></td>
<td>Similar to power-off, power-on reboot.</td>
<td>Quick restart.</td>
</tr>
<tr>
<td><strong>DHCP and TFTP Contact</strong></td>
<td>Contacts the DHCP server and TFTP server for their Cisco Unified CME system updates.</td>
<td>Does not contact the DHCP or TFTP server.</td>
</tr>
<tr>
<td><strong>Processing Time</strong></td>
<td>Takes longer to process when updating multiple phones.</td>
<td>Faster processing for multiple phones.</td>
</tr>
<tr>
<td><strong>When Required</strong></td>
<td>Must be used when updating the following:</td>
<td>Can be used when updating the following:</td>
</tr>
<tr>
<td></td>
<td>- Phone firmware</td>
<td>- Phone buttons</td>
</tr>
<tr>
<td></td>
<td>- User locale</td>
<td>- Phone lines</td>
</tr>
<tr>
<td></td>
<td>- Network locale</td>
<td>- Speed-dial numbers</td>
</tr>
<tr>
<td></td>
<td>- URL parameters</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Can be used when updating the following:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Phone buttons</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Phone lines</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Speed-dial numbers</td>
<td></td>
</tr>
</tbody>
</table>
### Task 8: Resetting and Restarting Phones

1. `exit`
2. `ephone phone-tag`
3. `reset`
4. `exit`

## DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
  - Enter your password if prompted. |
| **Example:** enabling router | Router> enable |
| **Step 2** configure terminal | Enters global configuration mode. |
| **Example:** enabling configuration terminal | Router# configure terminal |
| **Step 1** telephony-service | Enters telephony-service configuration mode. |
| **Example:** enabling telephony-service | Router(config)# telephony-service |
| **Step 2** reset {all [time-interval] | cancel  
  mac-address mac-address | sequence-all} | Performs a complete reboot of all phones or the phone with the specified MAC address, including contacting the DHCP and TFTP servers for the latest configuration information.  
  - **all**—Resets all phones associated with a Cisco Unified CME router. This keyword causes the router to pause 15 seconds between the reset start for each successive phone.  
  - **time-interval**—(Optional) Time interval, in seconds, between the start of each phone reset. Range is from 0 to 60. Default is 15.  
  - **cancel**—Interrupts a sequential reset cycle.  
  - **mac-address**—Resets the phone that has the specified MAC address.  
  - **sequence-all**—Resets all phones associated with this Cisco Unified CME router. This keyword causes the router to wait until one reset is complete before starting to reset the next phone. After the reset timeout of 4 minutes, the router stops waiting for the currently registering phone to complete registration and starts to reset the next phone. |
| **Example:** performing reset | Router(config-telephony)# reset all |
| **Step 3** exit | Exits telephony-service configuration mode. |
| **Example:** exiting configuration | Router(config-telephony)# exit |
Task 8: Resetting and Restarting Phones

Examples

The following example performs a complete reboot of ephone 1:

```
ephone 1
reset
```

The following example performs a complete sequential reboot of all phones associated with the router after the user locale code has been changed:

```
telephony-service
user-locale FR
reset sequence-all
```

Using the restart Command

The `restart` command is used to reboot IP phones after you make simple button, line, or speed-dial changes. A phone restart is faster than a phone reset because the DHCP and TFTP servers are not contacted for updates.

You can restart one phone or all phones from telephony-service configuration mode or you can restart a single phone from ephone configuration mode.

SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `telephony-service`
4. `restart {all [time-interval] | mac-address}`
5. `exit`
6. `ephone phone-tag`
7. `restart`
8. `exit`
**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> teledphone-service</td>
<td>Enters teledphone-service configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# teledphone-service</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> restart {all [time-interval]</td>
<td>mac-address}</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-telephony)# restart all</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> exit</td>
<td>Exits teledphone-service mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-telephony)# exit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> ephone phone-tag</td>
<td>Enters ephone configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# ephone 1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> restart</td>
<td>Performs a fast reboot of this ephone. Does not contact the DHCP or TFTP server for updated information.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-ephone)# restart</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong> exit</td>
<td>Exits ephone configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-ephone)# exit</td>
<td></td>
</tr>
</tbody>
</table>
Examples

The following example performs a fast reboot of ephone 1 after a change of button assignment:

ephone 1
button 1:32 2:33
restart

The following example performs a fast reboot of all phones associated with the router:

telephony-service
restart all

Task 9: Configuring Call Flows

After you have installed hardware and software, configured Cisco Unified CME parameters, provisioned phones, and reset phones, you can configure the other support and features that you need. Most important of this support is the call flow for your system. The following chapters describe features that are used to direct incoming and outgoing calls.

Also consult the Feature Map, page xxiii, for direct links to specific features.

- **Dial-Plan Support, page 113**—The `dialplan-pattern` command and voice translation rules both manipulate number patterns so that you can integrate an internal numbering scheme with external dialing patterns.

- **Call-Coverage Features, page 369**—Features include call forwarding, call hunt, call pickup, call waiting, ephone hunt groups, night service, and overlaid ephone-dns. Another call-coverage feature, Cisco Unified CME Basic Automatic Call Distribution and Auto-Attendant Service, is described in *Cisco Unified CME B-ACD and Tcl Call-Handling Applications*.

- **Call-Handling Features, page 443**—Features include call blocking based on date and time (after-hours toll bar), call hold, call park, call transfer, caller ID blocking, and conferencing.

Task 10: Adding Features

The following chapters provide configuration information for Cisco Unified CME features. Many of these features can be configured using the Cisco Unified CME GUI once it has been installed, as well by using as the Cisco IOS CLI.

Also consult the Feature Map, page xxiii, for direct links to specific features.

- **Cisco Unified CME GUI Support, page 123**—Use the GUI to provision phones and features after you have installed it and set up administrator and user accounts.

- **Phone Support, page 137**—Configurations for special phone types, including analog phones and Cisco IP Communicator.

- **Voice-Mail Support, page 299**—Procedures that support interworking with different voice-mail systems.

- **Phone Features, page 489**—Features related to answering phones and dialing (such as headset auto-answer and speed dial), phone displays (such as soft-key display), and phone functions (such as PC port disable and custom function buttons).
Administrative and System Features, page 313—Features include directories, ephone templates, ephone-dn templates, feature access codes, feature control, music on hold, paging, and timeouts and tones.

Configuration File Support, page 91—Externally stored and per-phone configuration files, alternative and user-defined user locales and network locales.

Task 11: Configuring Security for Phones

The following links provide information to make your Cisco Unified CME system more secure.

- Blocking automatic registration of ephones—The no auto-reg-ephone command, which is described in Step 7 of the “Task 5: Setting Cisco Unified CME Parameters” section on page 60, adds a level of security to your system. It blocks the automatic registration of ephones that do not have their MAC addresses explicitly listed in the configuration. Also see the “Blocking Automatic Registration: Example” section on page 69.
- Phone Authentication, page 149—Configuration information for secure SCCP signaling between Cisco Unified CME and Cisco Unified IP phones.

Task 12: Configuring Support for Multi-Site Functionality

The following chapters explain features that support a Cisco Unified CME system that covers multiple sites.

Also consult the Feature Map, page xxiii, for direct links to specific features.

- Trunking Support, page 263—Support includes direct FXO lines, QSIG supplementary services, and SIP trunks.
- Transcoding Support, page 199—Transcoding resources must be established when they are needed for packet conversions from one codec to another.
- Phone Support, page 137—Configurations for special phone types are covered, including teleworker remote phones.
- Transfer and Forwarding Support, page 223—Default Cisco Unified CME settings enable communications for call transfers and forwards across networks that use H.450 standards. This chapter explains alternatives for interworking with other transfer and forwarding situations.
Verifying the Cisco Unified CME Configuration

The following steps can be used to verify the Cisco Unified CME phone configurations.

SUMMARY STEPS

1. Use the `show running-config` command to verify ephone-dn configurations.
2. Verify the correct phone firmware installation by setting registration debugging with the `debug ephone register` command.
3. Use the `show telephony-service all` command to verify that the Cisco Unified CME router is enabled.
4. Use the `show telephony-service tftp-bindings` command to ensure that the locale-specific files are correct.
5. Use the `show ephone` command to verify Cisco Unified IP phone setup after phones have registered with the Cisco Unified CME router.
6. Use the `show ephone-dn` command to see settings related to ephone-dns.
7. Use the `show dialplan number` command to display the number resolutions of a particular phone number, which allows you to detect whether calls are going to unexpected destinations.

DETAILED STEPS

Step 1  Use the `show running-config` command to verify ephone-dn configurations.

```
ephone-dn 1
    number 1101
    name user1
    no huntstop
    call-forward noan 4000 timeout 30
  !
ephone-dn 2
    number 1101
    name user1
    preference 1
    call-forward busy 4000
    call-forward noan 4000 timeout 30
  !
ephone-dn 3
    number 1102
    name user2
    no huntstop
    call-forward noan 4000 timeout 30
  !
```

Step 2  Verify the correct phone firmware installation by setting registration debugging with the `debug ephone register` command. Then reset the phones and look at the StationAlarmMessage displayed during phone re-registration. The “Load=” parameter should appear in the display, followed by an abbreviated version name corresponding to the correct phone firmware filename.
Step 3  Use the `show telephony-service all` command to verify that the Cisco Unified CME router is enabled. This command also displays ephone-dn configurations.

```
Router# show telephony-service all
CONFIG (Version=4.0(0))
===================== Version 4.0(0)
Cisco Unified CallManager Express
For on-line documentation please see:
ip source-address 10.0.0.1 port 2000
max-ephones 24
max-dn 24
dialplan-pattern 1 408734....
voicemail 11111
transfer-pattern 510734....
keepalive 30
ephone-dn 1
   number 5001
   huntstop

ephone-dn 2
   number 5002
   huntstop
call-forward noan 5001 timeout 8
```

Step 4  Use the `show telephony-service tftp-bindings` command to ensure that the locale-specific files are correct.

```
Router# show telephony-service tftp-bindings
tftp-server system:/its/SEPDEFAULT.cnf
tftp-server system:/its/SEPDEFAULT.cnf alias SEPDefault.cnf
tftp-server system:/its/XMLDefault.cnf.xml alias XMLDefault.cnf.xml
tftp-server system:/its/XMLDefault7960.cnf.xml alias SEP00036B54BB15.cnf.xml
tftp-server system:/its/germany/7960-font.xml alias German_Germany/7960-font.xml
tftp-server system:/its/germany/7960-dictionary.xml alias German_Germany/SCCP-dictionary.xml
tftp-server system:/its/germany/7960-tones.xml alias Germany/7960-tones.xml
```

Step 5  Use the `show ephone [mac-address]` command to verify Cisco Unified IP phone setup after phones have registered with the Cisco Unified CME router.

```
Router# show ephone
mediaActive:0 offhook:0 ringing:0 reset:0 reset_sent:0 paging 0 debug:0
IP:20.0.0.2 51671 Telecaster 7940 keepalive 28 max_line 2
button 1: dn 1 number 4444 CM Fallback IDLE
ephone-2 Mac:0030.94C3.F43A TCP socket:[1] activeLine:0 REGISTERED
mediaActive:0 offhook:0 ringing:0 reset:0 reset_sent:0 paging 0 debug:0
IP:20.0.0.3 50994 Telecaster 7960 keepalive 28 max_line 6
button 1: dn 3 number 5555 CM Fallback IDLE
ephone-3 Mac:0003.6B40.99DA TCP socket:[3] activeLine:0 REGISTERED
mediaActive:0 offhook:0 ringing:0 reset:0 reset_sent:0 paging 0 debug:0
IP:1.2.168.200 51879 Telecaster 7960 keepalive 28 max_line 6
button 1: dn 2 number 3333 CM Fallback IDLE
Step 6  Use the `show ephone-dn` command to see settings related to an ephone-dn.

```
Router# show ephone-dn 7
50/0/7 INVALID
EFXS 50/0/7 Slot is 50, Sub-unit is 0, Port is 7
Type of VoicePort is EFXS
Operation State is UP
Administrative State is UP
No Interface Down Failure
Description is not set
Noise Regeneration is enabled
Non Linear Processing is enabled
Non Linear Mute is disabled
Non Linear Threshold is -21 dB
Music On Hold Threshold is Set to -38 dBm
In Gain is Set to 0 dB
Out Attenuation is Set to 0 dB
Echo Cancellation is enabled
Echo Cancellation NLP mute is disabled
Echo Cancellation NLP threshold is -21 dB
Echo Cancel Coverage is set to 8 ms
Playout-delay Mode is set to default
Playout-delay Nominal is set to 60 ms
Playout-delay Maximum is set to 200 ms
Playout-delay Minimum mode is set to default, value 4 ms
Playout-delay Fax is set to 300 ms
Connection Mode is normal
Connection Number is not set
Initial Time Out is set to 10 s
Interdigit Time Out is set to 10 s
Call Disconnect Time Out is set to 60 s
Ringing Time Out is set to 8 s
Wait Release Time Out is set to 30 s
Companding Type is u-law
Region Tone is set for US
Station name None, Station number None
Caller ID Info Follows:
Standard BELLCORE
Voice card specific Info Follows:
Digit Duration Timing is set to 100 ms
```

Step 7  Use the `show dialplan number` command to display the number resolutions of a particular phone number, which allows you to detect whether calls are going to unexpected destinations. This command is useful for troubleshooting cases in which you dial a number but the expected phone does not ring.
This section provides an example of the required Cisco Unified CME configuration with some of the additional options that are discussed in other chapters.

Router# show running-config

version 12.4
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname CME40
!
boot-start-marker
boot-end-marker
!
logging buffered 2000000 debugging
!
no aaa new-model
!
resource policy
!
clock timezone PST -8
clock summer-time PDT recurring
no network-clock-participate slot 2
voice-card 0
  no dspfarm
dsp services dspfarm
!
voice-card 2
dspfarm
!
no ip source-route
ip cef
!
!
!
!
ip domain name cisco.com
ip multicast-routing
!
!
ftp-server enable
ftp-server topdir flash:
isdn switch-type primary-5ess
!
!
!
voice service voip
  allow-connections h323 to sip
  allow-connections sip to h323
  no supplementary-service h450.2
  no supplementary-service h450.3
  h323
    call start slow
!
!
!
controller T1 2/0/0
framing esf
linecode b8zs
pri-group timeslots 1-24
!
controller T1 2/0/1
framing esf
linecode b8zs
!
!
!
!
!
!
!
!
!
!
!
interface GigabitEthernet0/0
ip address 192.168.1.1 255.255.255.0
ip pim dense-mode
duplex auto
speed auto
media-type rj45
negotiation auto
!
interface Service-Engine1/0
ip unnumbered GigabitEthernet0/0
service-module ip address 192.168.1.2 255.255.255.0
service-module ip default-gateway 192.168.1.1
!
interface Serial2/0/0:23
no ip address
encapsulation hdlc
isdn switch-type primary-5ess
isdn incoming-voice voice
isdn map address ^.* plan unknown type international
no cdp enable
!
ip route 0.0.0.0 0.0.0.0 192.168.1.254
ip route 192.168.1.2 255.255.255.255 Service-Engine1/0
ip route 223.255.254.253 255.255.255.255 1.2.0.1
ip route 223.255.254.254 255.255.255.255 1.2.0.1
!
ip http server
ip http authentication local
no ip http secure-server
ip http path flash:
tftp-server flash:P00307020300.loads
tftp-server flash:P00307020300.sb2
tftp-server flash:P00307020300.sbn

control-plane

voice-port 2/0/0:23

sccp local GigabitEthernet0/0
sccp ccm 192.168.1.1 identifier 1
sccp

sccp ccm group 1
associate ccm 1 priority 1
associate profile 1 register MTP0013c49a0cd0
keepalive retries 5

dspfarm profile 1 transcode
codec g711ulaw
codec g711alaw
codec g729ar8
codec g729abr8
codec gsmfr
codec g729r8
maximum sessions 90
associate application SCCP

dial-peer voice 9000 voip
mailbox-selection last-redirect-num
destination-pattern 78..
session protocol sipv2
session target ipv4:192.168.1.2
dtmf-relay sip-notify
codec g711ulaw
no vad

dial-peer voice 2 pots
incoming called-number .
direct-inward-dial
port 2/0/0:23
forward-digits all

dial-peer voice 1 pots
destination-pattern 9[2-9]......
port 2/0/0:23
forward-digits 8

dial-peer voice 3 pots
destination-pattern 91[2-9]..[2-9]......
port 2/0/0:23
forward-digits 12

gateway
timer receive-rtp 1200
telephony-service
load 7960-7940 P00307020300
max-phones 100
max-dn 300
ip source-address 192.168.1.1 port 2000
system message CCME 4.0
sdspfarm units 1
sdspfarm transcode sessions 128
sdspfarm tag 1 MTP0013c49a0cd0
voicemail 7800
max-conferences 24 gain -6
call-forward pattern .T
moh music-on-hold.au
multicast moh 239.1.1.1 port 2000
web admin system name admin password sjdfg
transfer-system full-consult
transfer-pattern .T
secondary-dialtone 9
create cnf-files version-stamp Jan 01 2002 00:00:00
ephone-dn-template 1
ephone-template 1
keep-conference endcall local-only
codec g729r8 dspfarm-assist
ephone-template 2
ephone-dn 1
number 6001
call-forward busy 7800
call-forward noan 7800 timeout 10
ephone-dn 2
number 6002
call-forward busy 7800
call-forward noan 7800 timeout 10
ephone-dn 10
number 6013
paging ip 239.1.1.1 port 2000
ephone-dn 20
number 8000....
mwi on
ephone-dn 21
number 8001....
mwi off
ephone 1
device-security-mode none
username "user1"
mac-address 002D.264E.54FA
codec g729r8 dspfarm-assist
type 7970
button 1:1

ephone 2
device-security-mode none
username "user2"
mac-address 001C.821C.ED23
type 7960
button 1:2

line con 0
stopbits 1
line aux 0
stopbits 1
line 66
no activation-character
no exec
transport preferred none
transport input all
transport output all
line 258
no activation-character
no exec
transport preferred none
transport input all
transport output all
line vty 0 4
eexec-timeout 0 0
privilege level 15
password sgpxw
login

scheduler allocate 20000 1000
ntp server 192.168.224.18

end
Configuration File Support

This chapter discusses the Cisco Unified CallManager Express (Cisco Unified CME) configuration files that the Cisco Unified IP phones use for information about how they should operate. It includes the following sections:

- Configuration File Support Overview, page 91
- Externally Stored and Per-Phone Configuration Files, page 93
- Alternative User and Network Locales, page 97
- User-Defined User and Network Locales, page 105


Configuration File Support Overview

Configuration files contain information that phones use for their operations.

Cisco ITS V2.1 introduced the use of XML configuration files for IP phones. There is one shared default XML configuration file for each type of IP phone. When an IP phone comes online or is rebooted, it automatically gets information about itself from the appropriate default configuration file. The phone coming online uses a filename alias based on the phone type, which either is automatically detected by the Cisco Unified CME router or is specified in the `type` command in `ephone` configuration mode. The `type` command is mandatory only for ATA phones or for IP phones that are adding one or two Cisco Unified IP Phone Expansion Module 7914s.

In Cisco ITS V2.1, Cisco CME 3.0, and later versions, the XML configuration files have been moved to `system:/its/`. The file named `flash:SEPDEFAULT.cnf` that was used with previous ITS versions is now obsolete, but is retained as `system:/its/SEPDEFAULT.cnf` to support upgrades from older phone firmware.

In a Cisco Unified CME system, the IP phones receive their initial configuration information and phone firmware from the TFTP server associated with the Cisco Unified CME router. In most cases, the phones obtain the IP address of their TFTP server using the Dynamic Host Configuration Protocol (DHCP) `option 150` command. For Cisco Unified CME operation, the TFTP server address obtained by the Cisco Unified IP phones should point to the Cisco Unified CME router IP address. The Cisco Unified IP phones attempt to transfer a configuration file called `XmlDefault.cnf.xml`. This file is automatically
Configuration File Support Overview

Configuration File Support

The ip source-address command generates the XMLDefault.cnf.xml file, which contains the IP address that the phones use to register for service, using the Skinny Client Control Protocol (SCCP). This IP address should correspond to a valid Cisco Unified CME router IP address (and may be the same as the router TFTP server address).

Similarly, when an analog telephone adaptor (ATA) such as the ATA-186 is attached to the Cisco Unified CME router, the ATA receives very basic configuration information and firmware from the TFTP server XMLDefault.cnf.xml file. Access to the XML Default.cnf.xml file must be granted by using the tftp-server command on the router. The XMLDefault.cnf.xml file is automatically generated by the Cisco Unified CME router with the ip source-address command and is placed in the router’s flash memory.

Cisco Unified CME 4.0 introduced the capability to use customized configuration files for individual phones or for phone type, in which you can select from up to five different user and network locales. Table 18 summarizes the configuration file topics discussed in this chapter.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Benefit</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Externally Stored and Per-Phone Configuration Files</td>
<td>System can store configuration files on an external TFTP server or other location and can specify a different configuration file per phone type or per individual phone.</td>
<td>Large configuration files don’t have to occupy flash memory space and you can apply different user and network locales per phone type or per phone.</td>
<td>A small business with a low-end router stores per-phone configuration files for each phone on an external TFTP server.</td>
</tr>
<tr>
<td>Alternative User and Network Locales</td>
<td>System can identify up to four alternative user and network locales in addition to a default.</td>
<td>Companies that need to support users in different locales can do so using a single Cisco Unified CME system.</td>
<td>A Cisco Unified CME system in Canada has some phones with US language and tones and others with French language and tones.</td>
</tr>
<tr>
<td>User-Defined User and Network Locales</td>
<td>System can create additional user and network locales using downloaded files.</td>
<td>Companies that need to support users in locales other than the currently offered locales are able to do so.</td>
<td>A business in China downloads files for traditional Chinese language and tones and identifies traditional Chinese as an alternative to their default locale.</td>
</tr>
</tbody>
</table>
Externally Stored and Per-Phone Configuration Files

This feature allows you to store phone configuration files in external locations and to apply them to individual phones or phone types. This section includes the following topics:

- Externally Stored and Per-Phone Configuration Files Overview, page 93
- Configuring Externally Stored and Per-Phone Configuration Files, page 95
- Verifying Externally Stored and Per-Phone Configuration Files, page 96
- Examples, page 97
- Feature History for Externally Stored and Per-Phone Configuration Files, page 97
- Related Features, page 97

Externally Stored and Per-Phone Configuration Files Overview

Note

For a summary of the functionality introduced in different releases, see the “Feature History for Externally Stored and Per-Phone Configuration Files” section on page 97.

In Cisco Unified CME 4.0 and later versions, you can use an external TFTP server to offload the TFTP server function on the Cisco Unified CME router. You can also use the slot 0 or flash memory on the Cisco Unified CME router for this purpose. This additional storage capacity provides the opportunity to use different configuration files for each phone type or for each phone, which allows you to specify different user locales and network locales for different phones. Prior to this release, you could specify only a single default user and network locale for a Cisco Unified CME system.

After using the steps in this task to create per-phone configuration files, you can perform the following additional tasks to customize user and network locales at your site:

- Create up to five user-defined user and network locales.
- Assign any of five different alternative user and network locales to individual phones using ephone templates. The alternative locales can be selected from the user-defined locales as well as from the locales that are already defined in the system (see CLI help for a list of available locales).

For more information on these tasks, see the “Alternative User and Network Locales” section on page 97 and the “User-Defined User and Network Locales” section on page 105.

You can specify any of the following four locations to store configuration files:

- System—This is the default. When the system is the storage location, there can be only one default configuration file and it is used for all phones in the system. All phones, therefore, use the same user locale and network locale. User-defined user and network locales are not supported. To use the system location, either do not use the `cnf-file location` command to specify a location or use the `no cnf-file location` command to reset the option from a previous, different location.

- Flash or slot 0—When flash or slot 0 memory on the router is the storage location, you can create additional configuration files that can be applied per phone type or per individual phone. Up to five user-defined user and network locales can be used in these configuration files. To store configuration files in flash or slot 0, use the `cnf-file location flash:` or `cnf-file location slot0:` command.
Note

When the storage location chosen is flash and the file system type on this device is Class B(LEFS), make sure to check free space on the device periodically and use the `squeeze` command to free the space used up by deleted files. Unless you use the `squeeze` command, the space used by the moved or deleted configuration files cannot be used by other files. Rewriting flash memory space during the `squeeze` operation may take several minutes. It is recommended that you use this command during scheduled maintenance periods or off-peak hours.

- TFTP—When an external TFTP server is the storage location, you can create additional configuration files that can be applied per phone type or per individual phone. Up to five user-defined user and network locales can be used in these configuration files. To store configuration files on an external TFTP server, use the `cnf-file location tftp url` command.

Configuration files are then applied in the following ways:

- Per system—This is the default. All phones use a single configuration file. The default user and network locale in a single configuration file are applied to all phones in the Cisco Unified CME system. Alternative and user-defined user and network locales are not supported. To use the per-system option, either do not use the `cnf-file` command or use the `no cnf-file` command to reset the option from a different configuration.

- Per phone type—This setting creates separate configuration files for each phone type. For example, all Cisco Unified IP Phone 7960s use XMLDefault7960.cnf.xml, and all Cisco Unified IP Phone 7905s use XMLDefault7905.cnf.xml. All phones of the same type use the same configuration file, which is generated using the default user and network locale. To create configuration files per phone type, use the `cnf-file perphonetype` command. This option is not supported if the location option is system.

- Per phone—This setting creates a separate configuration file for each phone, by MAC address. For example, a Cisco Unified IP Phone 7960 with the MAC address 123.456.789 creates the per-phone configuration file SEP123456789.cnf.xml. The configuration file for a phone is generated with the default user and network locale unless a different user and network locale is applied to the phone using an ephone template. To create configuration files per phone type, use the `cnf-file perphone` command. This option is not supported if the location option is system.

Restrictions

- Externally stored and per-phone configuration files are supported only on the following phones:
  - Cisco Unified IP Phones 7940 and 7940G
  - Cisco Unified IP Phones 7941G and 7941G-GE
  - Cisco Unified IP Phones 7960 and 7960G
  - Cisco Unified IP Phones 7961GT and 7961G-GE
  - Cisco Unified IP Phone 7970G
  - Cisco Unified IP Phone 7971G-GE

- TFTP does not support file deletion. When configuration files are updated, they overwrite any existing configuration files with the same name. If you change the configuration file location, files are not deleted from the TFTP server.

- The generation of configuration files on flash or slot 0 can take up to a minute, depending on the number of files that are being generated.
For smaller routers such as Cisco 2600 series routers, you must manually issue the `squeeze` command to erase files after changing the configuration file location or issuing any commands that trigger the deletion of configuration files. Unless you use the `squeeze` command, the space used by the moved or deleted configuration files cannot be used by other files.

**Configuring Externally Stored and Per-Phone Configuration Files**

This task allows you to specify a location to store configuration files and optionally to specify that configuration files should be unique per phone or phone type.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. telephony-service
4. cnf-file location {flash: | slot0: | tftp tftp-url}
5. cnf-file {perphonetype | perphone}

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3 telephony-service</td>
<td>Enters telephony-service configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# telephony-service</td>
<td></td>
</tr>
</tbody>
</table>
Configuration File Support

Externally Stored and Per-Phone Configuration Files

**Step 4**

```
cnf-file location {flash: | slot0: | tftp tftp-url}
```

**Purpose**

Specifies a location to store phone configuration files. The default is system. To reset the location to the default, use the `no` form of this command and the keyword that you previously used to set the location.

- **flash:** Router flash memory.
- **slot0:** Router slot 0 memory.
- **tftp tftp-url:** External TFTP server at a specified URL.

**Note**

When the storage location chosen is flash and the file system type on this device is Class B(LEFS), make sure to check free space on the device periodically and use the `squeeze` command to free the space used up by deleted files.

**Note**

When you change the configuration file storage location to TFTP or you change it from TFTP to something else, you must use the `option 150 ip` command address under the DHCP server configuration to update the address. For instructions, see the “Changing the TFTP Server Address” section on page 57. The router provides the following reminder prompt:

```
Router(config-telephony)# cnf-file location
TFTP tftp://10.1.100.175
Please update the options 150 configuration under ip dhcp pool. If the router is not the DHCP server, update the TFTP settings in the DHCP server.
```

**Step 5**

```
cnf-file {perphonetype | perphone}
```

**Purpose**

(Optional) Specifies whether to use a single configuration file for all phones, a separate file per type of phone, or a separate file for each individual phone. The default is to use a single configuration file for all phones.

- **perphonetype**—A separate configuration file is generated for each type of phone.
- **perphone**—A separate configuration file is generated for each phone.

**Note**

To reset the type of configuration file to the default, use the `no` form of this command and the keyword that you previously used to set the type.

---

**Verifying Externally Stored and Per-Phone Configuration Files**

**Step 1**

Use the `show telephony-service all` command to verify the settings for configuration file location and file generation option.
Examples

The following example selects flash memory as the configuration file storage location and per-phone as the type of configuration files that the system should generate.

telephony-service
    cnf-file location flash:
    cnf-file perphone

Feature History for Externally Stored and Per-Phone Configuration Files

<table>
<thead>
<tr>
<th>Cisco Unified CME Version</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.0</td>
<td>The ability to store configuration files externally and apply them per phone or phone type was introduced.</td>
</tr>
</tbody>
</table>

Related Features

Alternative User and Network Locales

After you have defined new user and network locales, you can assign them as alternative locales. For more information, see the “Alternative User and Network Locales” section on page 97.

User-Defined User and Network Locales

You can download files to define more user and network locales than those already available in the system. For more information, see the “User-Defined User and Network Locales” section on page 105.

Alternative User and Network Locales

This feature allows you to define several user and network locales as alternatives to the default and apply them to individual phones. This section contains the following topics:

- Alternative User and Network Locales Overview, page 98
- Configuring Alternative User and Network Locales, page 99
- Verifying Alternative User and Network Locales, page 102
- Examples, page 102
- Troubleshooting Alternative User and Network Locales, page 104
- Feature History for Alternative User and Network Locales, page 104
- Related Features, page 104
Alternative User and Network Locales Overview

Note
For a summary of the functionality introduced in different releases, see the “Feature History for Alternative User and Network Locales” section on page 104.

The addition of per-phone configuration files in Cisco Unified CME 4.0 and later versions allows you to specify alternative user locales and network locales for individual phones or for groups of phones using ephone-templates.

Prior to Cisco Unified CME 4.0, only one user locale and one network locale could be specified for all phones in a Cisco Unified CME system. The language tag argument in the `user-locale` command allows you to specify up to five alternative user locales for use in a Cisco Unified CME system. For example, a company can specify user-locale French for phones A, B, and C; user-locale German for phones D, E, and F; and user-locale United States for phones G, H, and I. The locale-tag argument in the `network-locale` command allows you to do the same thing for network locales.

Each one of the five alternative user locales and network locales that you can define in a multi-locale system is identified with a language tag identifier. The identifier 0 always holds the default locale, although you can define this default to be any language code that is supported in the system and is listed in the CLI help for the command. For example, if you define user locale 0 to be JP (Japanese), the default user locale for the router is JP. If you do not specify a locale for the identifier 0, the default is US (United States).

To apply alternative user locales to different phones, you must also use the `cnf-files` command to specify per-phone configuration files. When per-phone is specified, individual configuration files are built for each phone. The configuration files automatically use the default locales in user-locale 0 and network-locale 0. You can override these defaults for individual phones by assigning alternative language tag identifiers to the alternative locale codes that you want to use and then creating ephone-templates to assign the alternative language tag identifiers to individual phones.

After using the `user-locale (telephony-service)` command to associate a language tag identifier with a language code, use the `user-locale` command in ephone-template mode to apply this number to an ephone template. Then use the `ephone-template` command in ephone configuration mode to apply the template to one or more ephones. An example is shown in the “Examples” section on page 102. For ephone-template configuration instructions, see the “Ephone Templates” section on page 318.

Prerequisites

- To specify alternative user and network locales for individual phones in a Cisco Unified CME system, per-phone configuration files must be used. For more information, see the “Externally Stored and Per-Phone Configuration Files” section on page 93.
- You can also use user-defined, non-supported locale codes as alternative locales, but you must first download the appropriate XML files. See the “User-Defined User and Network Locales” section on page 105.
Restrictions

- Alternative user and network locales are supported only on the following phones:
  - Cisco Unified IP Phones 7940 and 7940G
  - Cisco Unified IP Phones 7941G and 7941G-GE
  - Cisco Unified IP Phones 7960 and 7960G
  - Cisco Unified IP Phones 7961G and 7961G-GE
  - Cisco Unified IP Phone 7970G
  - Cisco Unified IP Phone 7971G-GE

- When you use the setup tool from the telephony-service setup command to provision phones, you can only choose a default user locale and network locale, and you are limited to selecting a locale code that is provided in the system. You cannot use alternative or user-defined locales with the setup tool.

Configuring Alternative User and Network Locales

This task identifies one or more alternatives to the default user and network locale and applies them to individual ephones.

SUMMARY STEPS

1. enable
2. configure terminal
3. telephony-service
4. user-locale [language-tag] language-code
5. network-locale [locale-tag] locale-code
6. create cnf-files
7. exit
8. ephone-template template-tag
9. user-locale language-tag
10. network-locale locale-tag
11. exit
12. ephone phone-tag
13. ephone-template template-tag
14. exit
15. telephony service
16. reset {all [time-interval] | cancel | mac-address mac-address | sequence-all}
17. exit
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>enable</strong>&lt;br&gt;Enables privileged EXEC mode.&lt;br&gt;  - Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router&gt; enable</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>configure terminal</strong>&lt;br&gt;Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router# configure terminal</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>telephony-service</strong>&lt;br&gt;Enters telephony-service configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config)# telephony-service</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><strong>user-locale [language-tag] language-code</strong>&lt;br&gt;Specifies a language for phone displays. If you use the language-tag argument, you also use the user-locale command in ephone or ephone-template configuration mode to apply the language tag to individual ephones. If you do not use the language-tag argument, the language code you specify becomes the default and is applied to all ephones.&lt;br&gt;  - language-tag—(Optional) Assigns a language tag identifier to the language code that follows. Range is 0 to 4. The default is 0.&lt;br&gt;  - language-code—Refer to CLI help for a list of ISO-3166 codes that are supported. United States (US) is the default.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-telephony)# user-locale 1 FR</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><strong>network-locale [language-tag] language-code</strong>&lt;br&gt;Specifies a language for phone displays. If you use the language-tag argument, you also use the user-locale command in ephone or ephone-template configuration mode to apply the language tag to individual ephones. If you do not use the language-tag argument, the language code you specify becomes the default and is applied to all ephones.&lt;br&gt;  - language-tag—(Optional) Assigns a language tag identifier to the language code that follows. Range is 0 to 4. The default is 0.&lt;br&gt;  - language-code—Refer to CLI help for a list of ISO-3166 codes that are supported. United States (US) is the default.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-telephony)# user-locale 1 FR</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><strong>create cnf-files</strong>&lt;br&gt;BUILDS THE XML CONFIGURATION FILES THAT ARE REQUIRED FOR IP PHONES. USE THIS COMMAND AFTER YOU UPDATE CONFIGURATION FILE PARAMETERS SUCH AS USER LOCALE OR NETWORK LOCALE.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-telephony)# create cnf-files</td>
</tr>
</tbody>
</table>
### Command or Action | Purpose
--- | ---
Step 7  
**exit**  
Example:  
Router(config-telephony)# exit  
| Exits telephony-service configuration mode. |
Step 8  
**ephone-template**  
*template-tag*  
Example:  
Router(config)# ephone-template  
| Enters ephone-template configuration mode. |
Step 9  
**user-locale**  
*language-tag*  
Example:  
Router(config-ephone-template)# user-locale  
| Applies the specified language tag to the ephone-template that is being defined.  
  * language-tag—A language tag identifier that was defined in Step 4. |
Step 10  
**network-locale**  
*locale-tag*  
Example:  
Router(config-ephone-template)# network-locale  
| Applies the specified locale tag to the ephone-template that is being defined.  
  * locale-tag—A locale tag identifier that was defined in Step 5. |
Step 11  
**exit**  
Example:  
Router(config-ephone-template)# exit  
| Exits ephone-template configuration mode. |
Step 12  
**ephone**  
*phone-tag*  
Example:  
Router(config)# ephone  
| Enters ephone configuration mode.  
  * phone-tag—Unique sequence number that identifies this ephone during configuration tasks. |
Step 13  
**ephone-template**  
*template-tag*  
Example:  
Router(config-ephone)# ephone-template  
| Applies an ephone template to an ephone. |
Step 14  
**exit**  
Example:  
Router(config-ephone)# exit  
| Exits ephone configuration mode. |
Step 15  
**telephony-service**  
Example:  
Router(config)# telephony-service  
| Enters telephony-service configuration mode. |
Verifying Alternative User and Network Locales

Step 1

Use the `show running-config` command to display the running configuration. Review the telephony-service portion of the output for alternative locales, the ephone portion to see which templates are applied to which ephones, and the ephone-template portion for the contents of ephone templates.

Examples

The following example sets the default value of 0 to Germany, which defines Germany as the default user and network locale. Germany will be used for all phones in the system unless a different locale is applied to individual phones using ephone templates.

```
telephony service
cnf-file location flash:
cnf-file perphone
user-locale 0 DE
network-locale 0 DE
```

After using the previous commands to define Germany as the default user and network locale, you use the following commands if you want to return the default value of 0 to US:

```
telephony service
no user-locale 0 DE
no network-locale 0 DE
```
Another way to define Germany as the default user and network locale is to use the following commands:

```
telephony service
cnf-file location flash:
cnf-file perphone
user-locale DE
network-locale DE
```

After using the previous commands, you use the following commands if you want to return the default to US:

```
telephony service
no user-locale DE
no network-locale DE
```

The following example defines three alternative locales: JP (Japan), FR (France), and ES (Spain). The default is US for all phones that do not have the alternatives applied using ephone templates. In this example, ephone 11 uses JP for its locales, ephone 12 uses FR, ephone 13 uses ES, and ephone 14 uses the default, US.

```
telephony-service
cnf-file location flash:
cnf-file perphone
create cnf-files
user-locale 1 JP
user-locale 2 FR
user-locale 3 ES
network-locale 1 JP
network-locale 2 FR
network-locale 3 ES
create cnf-files
ephone-template 1
user-locale 1
network-locale 1
ephone-template 2
user-locale 2
network-locale 2
ephone-template 3
user-locale 3
network-locale 3
ephone 11
button 1:25
ephone-template 1
ephone 12
button 1:26
ephone-template 2
ephone 13
button 1:27
ephone-template 3
ephone 14
button 1:28
```
Troubleshooting Alternative User and Network Locales

Step 1  Use the show telephony-service tftp-bindings command to display list of configuration files that are accessible to IP phones using TFTP, including the dictionary, language, and tone configuration files.

Router(config)# show telephony-service tftp-bindings

tftp-server system:/its/SEPDEFAULT.cnf
 tftp-server system:/its/SEPDEFAULT.cnf alias SEPDefault.cnf
 tftp-server system:/its/XMLDefault.cnf.xml alias XMLDefault.cnf.xml
 tftp-server system:/its/XMLDefault.cnf.xml alias XMLDefault.cnf.xml
 tftp-server system:/its/XMLDefault7960.cnf.xml alias SEP00036B54BB15.cnf.xml
 tftp-server system:/its/germany/7960-font.xml alias German_Germany/7960-font.xml
 tftp-server system:/its/germany/7960-dictionary.xml alias German_Germany/7960-dictionary.xml
 tftp-server system:/its/germany/7960-dictionary.xml alias Germany/7960-dictionary.xml
 tftp-server system:/its/germany/7960-tones.xml alias Germany/7960-tones.xml

Feature History for Alternative User and Network Locales

<table>
<thead>
<tr>
<th>Cisco Unified CME Version</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.0</td>
<td>Alternative user and network locales were introduced.</td>
</tr>
</tbody>
</table>

Related Features

Ephone Templates
For more information about ephone templates, see the “Ephone Templates” section on page 318.

Per-Phone Configuration Files
For more information about per-phone configuration files, see the “Externally Stored and Per-Phone Configuration Files” section on page 93.

User-Defined User and Network Locales
You can download files to define more user and network locales than those already available in the system. For more information, see the “User-Defined User and Network Locales” section on page 105.
User-Defined User and Network Locales

This feature allows you to specify user and network locales in addition to those that are provided in the Cisco Unified CME system and then apply them to individual ephones. This section includes the following topics:

- User-Defined User and Network Locales Overview, page 105
- Configuring User-Defined User and Network Locales, page 106
- Verifying User-Defined User and Network Locales, page 109
- Examples, page 110
- Troubleshooting User-Defined User and Network Locales, page 111
- Feature History for User-Defined User and Network Locales, page 111
- Related Features, page 111

User-Defined User and Network Locales Overview

Note

For a summary of the functionality introduced in different releases, see the “Feature History for User-Defined User and Network Locales” section on page 111.

Cisco Unified CME today offers internal localization support for 12 languages including English, which provides a method to support additional localizations from other Cisco call processing systems for use with Cisco Unified CME.

For example, Cisco Unified CME has preloaded a number of common user locales and network locales into the system. By using CLI help, you can view the list of the provided locales and their two-letter codes. However, you may have need for locales other than the supported locales. This section explains how to define and implement other locales.

Cisco provides XML files for user locales and network locales that are not currently provided in the system. Beginning in Cisco Unified CME 4.0, you can install the files to add a particular user and network locale in slot 0, flash, or external TFTP memory. Note that these files cannot be installed in the system location. The user-locale and network-locale files that are stored in this fashion can then be used as default or alternative locales for all or some phones.

For example, you have a site at which the phones should use the displays and tones for Traditional Chinese, which is not one of the supported choices in Cisco Unified CME. You complete the following steps to install Traditional Chinese on the phones that need this locale.

1. Download the correct files and copy them to slot 0, flash, or TFTP.
2. Specify per-phone as the method for assigning configuration files.
3. Assign user and network locale tags and a user-defined code (U1 to U5) to the locale code you want to use. Locale codes are based on the ISO 639 list, which is available at the Library of Congress website: http://www.loc.gov/standards/iso639-2/.
4. Rebuild the configuration files.
5. Create an ephone template that contains the user and network locale tags.
6. Apply the ephone template to the ephones that need the Traditional Chinese display and tones.
7. Reset the phones.
Prerequisites

- Per-phone configuration files must be created as described in the “Externally Stored and Per-Phone Configuration Files” section on page 93.
- XML files for the non-supported locale that you want to use must be downloaded and copied to an appropriate storage location: slot 0, flash, or TFTP. Note that you cannot use the system location for user-defined locale files.

Restrictions

- User-defined user and network locales are supported only on the following phones:
  - Cisco Unified IP Phone 7905G
  - Cisco Unified IP Phone 7912G
  - Cisco Unified IP Phone 7940G
  - Cisco Unified IP Phone 7960G
- User-defined user locales and network locales are not supported if the configuration file location is system.
- When you use the setup tool from the `telephony-service setup` command to provision phones, you can only choose a default user locale and network locale, and you are limited to selecting a locale code that is supported in the system. You cannot use alternative or user-defined locales with the setup tool.
- When a user-defined user locale is used, the phone display normally displays text using the user-defined fonts, except for any strings that are interpreted by Cisco Unified CME, such as “Cisco/Personal Directory,” “Speed Dial/Fast Dial,” and so forth.

Configuring User-Defined User and Network Locales

This task defines custom user and network locales and applies them to individual phones.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `telephony-service`
4. `user-locale [language-tag [user-defined-code]] language-code`
5. `network-locale [network-locale-tag [user-defined-code]] locale-code`
6. `create cnf-files`
7. `exit`
8. `ephone-template template-tag`
9. `user-locale language-tag`
10. `network-locale network-locale-tag`
11. `exit`
12. `ephone phone-tag`
13. **ephone-template** *template-tag*
14. **exit**
15. **telephony service**
16. **reset** `{all [time-interval] | cancel | mac-address mac-address | sequence-all}`
17. **exit**

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1 enable</strong></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Enter your password if prompted.</td>
</tr>
<tr>
<td></td>
<td>.Router&gt; enable</td>
</tr>
<tr>
<td><strong>Step 2 configure terminal</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>.Router# configure terminal</td>
</tr>
<tr>
<td><strong>Step 3 telephony-service</strong></td>
<td>Enters telephony-service configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>.Router(config)# telephony-service</td>
</tr>
<tr>
<td><strong>Step 4 user-locale</strong></td>
<td>Specifies a language for phone displays. If you use the language-tag argument, you must also use the user-locale command in ephone or ephone-template configuration mode to apply the language tag to individual phones. If you do not use the language-tag argument, the language code is applied to all ephones.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>.Router(config-telephony)# user-locale 1 U1 ZH</td>
</tr>
</tbody>
</table>
### Command or Action

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| 5      | `network-locale [locale-tag [user-defined-code]] locale-code` | Specifies a locale for tones. If you use the `locale-tag` argument, you must also use the `network-locale` command in ephone or ephone-template configuration mode to apply the language tag to individual phones. If you do not use the `language-tag` argument, the language code is applied to all ephones.  
- `locale-tag`—(Optional) Assigns a locale tag identifier to the user-defined code that follows. Range is 0 to 4.  
- `user-defined-code`—(Optional) Assigns one of the user-defined codes to the specified locale code.  
- `locale-code`—Refer to CLI help for a list of ISO-3166 codes that are supported. United States (US) is the default. |
| 6      | `create cnf-files`             | Builds the XML configuration files that are required for IP phones. Use this command after you update configuration file parameters such as user locale or network locale. |
| 7      | `exit`                                | Exits telephony-service configuration mode.                           |
| 8      | `ephone-template template-tag`     | Enters ephone-template configuration mode.                            |
|        |                                        | - `template-tag`—Unique sequence number that identifies this template during configuration tasks. |
| 9      | `user-locale language-tag`          | Assigns a user locale to this ephone template.                         |
|        |                                        | - `language-tag`—A language tag that was created in Step 4. Range is 0 to 4. |
| 10     | `network-locale locale-tag`         | Assigns a network locale to this ephone template.                      |
|        |                                        | - `locale-tag`—A locale tag that was created in Step 5. Range is 0 to 4. |
| 11     | `exit`                                | Exits ephone-template configuration mode.                             |
| 12     | `ephone phone-tag`                  | Enters ephone configuration mode.                                      |
|        |                                        | - `phone-tag`—Unique sequence number that identifies this ephone during configuration tasks. |
Configuration File Support

User-Defined User and Network Locales

Verifying User-Defined User and Network Locales

Step 1 Use the show running-config command to display the running configuration. Review the ephone portion to see which templates are applied to which ephones, and the ephone-template portion for the contents of ephone templates.
Examples

The following example applies the alternative language tag 4 to the user-defined code U1, which is defined as ZH for Traditional Chinese by ISO 639, Language Code Reference. The code for Traditional Chinese is not one of those that have been preloaded in the system, so the user must download the appropriate XML files to support this language.

The example also defines three other alternative locales: JP (Japan), FR (France), and ES (Spain). The default is US for all phones that do not have the alternatives applied using ephone templates. In this example, ephone 11 uses JP for its locales, ephone 12 uses FR, ephone 13 uses ES, ephone 14 uses the default, US, and ephone 15 uses the user-defined language, ZH (Traditional Chinese).

telephony-service
cnf-file location flash:
cnf-file perphone
user-locale 1 JP
user-locale 2 FR
user-locale 3 ES
user-locale 4 U1 ZH
network-locale 1 JP
network-locale 2 FR
network-locale 3 ES
network-locale 4 U1 ZH

ephone-template 1
user-locale 1
network-locale 1

ephone-template 2
user-locale 2
network-locale 2

ephone-template 3
user-locale 3
network-locale 3

ephone-template 4
user-locale 4
network-locale 4

ephone 11
button 1:25
ephone-template 1

ephone 12
button 1:26
ephone-template 2

ephone 13
button 1:27
ephone-template 3

ephone 14
button 1:28

ephone 15
button 1:29
ephone-template 4
Troubleshooting User-Defined User and Network Locales

Step 1  Make sure that you have defined per-phone configuration files.
Step 2  Use the `show telephony-service ephone-template` command to check the user locale and network locale settings in each ephone template.
Step 3  Use the `show telephony-service ephone` command to check that the correct templates are applied to phones.
Step 4  Use the show `telephony-service tftp-bindings` command to display the current configuration files that are accessible to IP phones.

Feature History for User-Defined User and Network Locales

<table>
<thead>
<tr>
<th>Cisco Unified CME Version</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.0</td>
<td>User-defined user and network locales were introduced.</td>
</tr>
</tbody>
</table>

Related Features

**Ephone Templates**
For more information about ephone templates, see the “Ephone Templates” section on page 318.

**Per-Phone Configuration Files**
For more information about per-phone configuration files, see the “Externally Stored and Per-Phone Configuration Files” section on page 93.

**Alternative User and Network Locales**
After you have defined new user and network locales, you can assign them as alternative locales. For more information, see the “Alternative User and Network Locales” section on page 97.
Dial-Plan Support

This chapter describes Cisco Unified CallManager Express (Cisco Unified CME) features that expand or manipulate internal extension numbers so that they conform to numbering plans used by external systems. It contains the following sections:

- Dial-Plan Support Overview, page 113
- Dial-Plan Patterns, page 114
- Voice Translation Rules and Profiles, page 117

Note

Dial-Plan Support Overview

Dial-plan support features allow you to expand or manipulate extension numbers to integrate with numbering plans used by external systems with which you interface. Table 19 summarizes the features.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Benefit</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Dial-Plan Patterns</strong></td>
<td>System adds a prefix to extensions to transform them into E.146 numbers.</td>
<td>Phone users can dial short extension numbers for internal calls and can make and receive external calls.</td>
<td>A customer service desk can be reached internally by dialing 156, and externally by dialing 555-0156.</td>
</tr>
<tr>
<td><strong>Voice Translation Rules and Profiles</strong></td>
<td>System adds, removes, or transforms digits for calls going to or originating from specified ephone-dns.</td>
<td>Internal and external dial plans appear seamless. Translation profiles provide ease of configuration.</td>
<td>An employee dials a 5-digit extension to reach a phone at another site. If the call is routed through the PSTN, the originating gateway must use translation rules to convert the 5-digit extension into a 10-digit format that is recognized by the central office switch.</td>
</tr>
</tbody>
</table>
Dial-Plan Patterns

A dial-plan pattern creates a sequence of digits that specifies a global prefix for the expansion of abbreviated extension numbers into fully qualified E.164 numbers. This section includes the following topics:

- Dial-Plan Patterns Overview, page 114
- Configuring Dial-Plan Patterns, page 115
- Verifying Dial-Plan Patterns, page 117
- Examples, page 117
- Troubleshooting Dial-Plan Patterns, page 117
- Feature History for Dial-Plan Patterns, page 117

Dial-Plan Patterns Overview

For a summary of the functionality introduced in different releases, see the “Feature History for Dial-Plan Patterns” section on page 117.

The `dialplan-pattern` command creates a sequence of digits that specifies a global prefix for the expansion of abbreviated extension numbers into fully qualified E.164 numbers. You can define up to five dial-plan patterns.

In networks that have a single router, you do not need to use the `dialplan-pattern` command.

If multiple dial-plan patterns are defined, the system matches extension numbers against the patterns in sequential order, starting with the pattern that was defined first. Once a pattern matches an extension number, the pattern is used to generate an expanded number. If additional patterns subsequently match the extension number, they are not used.

The `dialplan-pattern` command builds additional dial peers for the expanded numbers it creates. For example, when the ephone-dn with the number 1001 was defined, the following POTS dial peer was automatically created for it:

```
dial-peer voice 20001 pots
  destination-pattern 1001
  voice-port 50/0/2
```

If you then define a dial-plan pattern that 1001 will match, such as 4085551001, a second dial peer is created so that calls to both the 1001 and 4085551001 numbers will be completed. Both dial peers can be seen with the `show telephony-service dial-peer` command. In this example, the additional dial peer that is automatically created by the `dialplan-pattern` command looks like the following:

```
dial-peer voice 20002 pots
  destination-pattern 4085551001
  voice-port 50/0/2
```

In networks with multiple routers, you may need to use the `dialplan-pattern` command to expand extensions to E.164 numbers because local extension numbering schemes can overlap each other. Networks with multiple routers have authorities such as gatekeepers that route calls through the network. These authorities use require E.164 numbers so that all numbers in the network will be unique. The `dialplan-pattern` command expands extension numbers into unique E.164 numbers for that use.
A dial-plan pattern is required to register the Cisco Unified IP phone lines with a gatekeeper. Ephone-dn numbers for the Cisco Unified IP phones must match the number in the extension-length argument. For example, if the extension length is 3, all extensions must be three numbers in length. Otherwise, the extension number cannot be converted to a qualified E.164 number.

Using the dialplan-pattern command to expand extension numbers can sometimes result in the improper matching of numbers with dial peers. For example, the expanded E.164 number 2035550134 matches dial-peer destination-pattern 203, not 134, which would be the correct destination pattern for the desired extension.

If it is necessary for you to use the dialplan-pattern command and you know that the expanded numbers might match destination patterns for dial peers, you can manually configure an extension’s E.164 expanded number as its secondary number instead of using the dialplan-pattern command, as shown in the following example.

```
ephone-dn 23
  number 134 secondary 2035550134
```

The pattern created by the dialplan-pattern command is also used to enable distinctive ringing for inbound calls. If a calling-party number matches a dial-plan pattern, the call is considered an internal call and has a distinctive ring that identifies the call as internal. Any call with a calling-party number that does not match a dial-plan pattern is considered an external call and has a distinctive ring that is different from the internal ringing.

When the extension-pattern keyword and extension-length argument are used, the leading digits of an extension pattern are stripped and replaced with the corresponding leading digits of the dial plan. For example, the following command maps all 4xx extension numbers to the PSTN number 40855501xx, so that extension 412 corresponds to 4085550112.

```
dialplan-pattern 1 4085550100 extension-length 3 extension-pattern 4..
```

The extension-pattern keyword allows additional manipulation of abbreviated extension-number prefix digits. When this keyword and its argument are used, the leading digits of an extension pattern are stripped and replaced by the corresponding leading digits of the dial-plan pattern. This command can be used to avoid having Direct Inward Dialing (DID) numbers like 408-555-0101 result in four-digit extensions such as 0101.

### Configuring Dial-Plan Patterns

This procedure sets up a dial-plan pattern.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `telephony-service`
4. `dialplan-pattern tag pattern extension-length length [extension-pattern epattern] [no-reg]`
5. `exit`
## DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** `enable` | Enables privileged EXEC mode.  
  - Enter your password if prompted. |
| **Example:** Router> enable | |
| **Step 2** `configure terminal` | Enters global configuration mode. |
| **Example:** Router# configure terminal | |
| **Step 3** `telephony-service` | Enters telephony-service configuration mode. |
| **Example:** Router(config)# telephony-service | |
| **Step 4** `dialplan-pattern` `tag` `pattern` `extension-length` `length`  
  `[extension-pattern` `epattern]` `[no-reg]` | Maps a digit pattern for an abbreviated extension-number prefix to the full E.164 telephone number pattern.  
  - `tag`—Dial-plan string tag used before a ten-digit telephone number. Range is from 1 to 5.  
  - `pattern`—Dial-plan pattern for full E.164 number.  
  - `extension-length` `length`—Number of digits in the `epattern` argument that is associated with the `extension-pattern` keyword.  
  - `extension-pattern` `epattern`—(Optional) Internal extension pattern to use. In addition to digits, the following wildcards can be used:  
    - . (period)—Stands for a single character.  
    - T—Stands for timeout in the context of the user entering digits. For example, four periods and a T (. . . .T) tells the system to receive at least four digits from the user and wait for the user to stop entering digits.  
  - `no-reg`—(Optional) Prevents the E.164 number in the dial peer from registering with a gatekeeper. By not registering some numbers, you leave them available to be used for other telephony services. |
| **Example:** Router(config-telephony)# dialplan-pattern 1 4085550100 extension-length 3 extension-pattern 4.. | |
| **Note** | This example maps all extension numbers 4xx to the PSTN number 40855501xx, so that extension 412 corresponds to 4085550112. |
| **Step 5** `exit` | Exits telephony-service configuration mode. |
| **Example:** Router(config-telephony)# exit | |
Verifying Dial-Plan Patterns

Step 1 Use the `show running-config` command or the `show telephony-service` command to verify dial-plan patterns in the configuration.

Examples

The following example maps the extension pattern 4.. to the last three digits of the dial-plan pattern 4085550155:

```
telephony-service
dialplan-pattern 1 4085550155 extension-length 3 extension-pattern 4..
```

Troubleshooting Dial-Plan Patterns

Step 1 Use the `show telephony-service dial-peer` command to display dial peers that are automatically created by the `dialplan-pattern` command.

Feature History for Dial-Plan Patterns

<table>
<thead>
<tr>
<th>Cisco Unified CME Version</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>The ability to manipulate numbers to conform to internal or external numbering patterns was introduced.</td>
</tr>
<tr>
<td>2.1</td>
<td>The <code>extension-pattern</code> keyword was added to the <code>dialplan-pattern</code> command.</td>
</tr>
</tbody>
</table>

Voice Translation Rules and Profiles

Voice translation rules manipulate dialed numbers to conform to internal or external numbering schemes. Voice translation profiles allow you to group rules together. This section includes the following topics:

- Voice Translation Rules and Profiles Overview, page 118
- Configuring Voice Translation Rules and Profiles, page 118
- Verifying Voice Translation Rules and Profiles, page 120
- Examples, page 121
- Troubleshooting Voice Translation Rules and Profiles, page 121
- Feature History for Voice Translation Rules and Profiles, page 121
- Related Features, page 122
Voice Translation Rules and Profiles Overview

For a summary of the functionality introduced in different releases, see the “Feature History for Voice Translation Rules and Profiles” section on page 121.

Cisco CME 3.2 and later versions support voice translation rules and voice translation profiles. Voice translation rules perform manipulations on numbers. Voice translation profiles allow you to group voice translation rules together and associate them with the following:

- Called numbers
- Calling numbers
- Redirected called numbers

Note

Voice translation rules supersede an older implementation of translation rules, which are still supported in Cisco Unified CME 4.0 for backward compatibility. For information about the previous implementation of translation rules, see the “Translation Rules” section in the “Setting Up Phones” chapter of the Cisco CME 3.3 System Administrator Guide.

Voice translation rules have the ability to perform regular expression matches and replace substrings. The Stream EDitor (SED) utility is used to translate numbers. The translation rules replace a substring of the input number if the number matches the match pattern, number plan, and type present in the rule. The SED utility is used to check for a match based on the match pattern.

Voice translation profiles are created and named with the voice translation-profile command. In the translation-profile configuration mode, the translate command is used to associate translation rules with the translation profile and to associate the translation rules with called numbers, calling numbers, or redirected called numbers. Finally, translation profiles are added to ephone-dn configurations using the translation-profile command. The incoming keyword changes the parameters of calls that come from the IP phone. The outgoing keyword changes the values of calls that go out of the router to the IP phone.

For examples of voice translation rules and profiles, see the “Voice Translation Rules” technical note and the “Number Translation using Voice Translation Profiles” technical note.

Configuring Voice Translation Rules and Profiles

This task sets up a translation profile and applies it to an ephone-dn.

SUMMARY STEPS

1. enable
2. configure terminal
3. voice translation-rule number
4. rule precedence /match-pattern/ /replace-pattern/
5. exit
6. voice translation-profile name
7. translate {called | calling | redirect-called} voice-translation-rule-tag
8. exit
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| 1.   | enable            | Enables privileged EXEC mode.  
        |                   | - Enter your password if prompted. |
| 2.   | configure terminal| Enters global configuration mode. |
| 3.   | voice translation-rule number | Defines a translation rule for voice calls and enters voice translation-rule configuration mode.  
        |                   | - **number**—Number that identifies the translation rule. Range is from 1 to 2,147,483,647. |
| 4.   | rule precedence /match-pattern/ /replace-pattern/ | Defines a translation rule.  
        |                   | - **precedence**—Priority of the translation rule. Range is from 1 to 15.  
        |                   | - **match-pattern**—Stream editor (SED) expression used to match incoming call information. The slash (/) is a delimiter in the pattern.  
        |                   | - **replace-pattern**—SED expression used to replace the match pattern in the call information. The slash (/) is a delimiter in the pattern. |
| 5.   | exit              | Exits voice translation-rule configuration mode. |
| 6.   | voice translation-profile name | Defines a translation profile for voice calls.  
        |                   | - **name**—Name of the translation profile. Maximum length of the voice translation profile name is 31 alphanumeric characters. |
## Verifying Voice Translation Rules and Profiles

### Step 1
Use the `show running-config` command to display translation profiles and whether they have been applied to the appropriate ephone-dn.

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 7</strong></td>
<td></td>
</tr>
</tbody>
</table>
| `translate {called | calling | redirect-called}` voice-translation-rule-tag | Associates a voice translation rule with a voice translation profile.  
  - `called`—Associates the translation rule with called numbers.  
  - `calling`—Associates the translation rule with calling numbers.  
  - `redirect-called`—Associates the translation rule with redirected called numbers.  
  - `translate-rule-tag`—Reference number of the translation rule. Range is from 1 to 2147483647. |
| **Example:** | |
| `Router(cfg-translation-profile)# translate called 1` | |
| **Step 8**        |         |
| `exit` | Exits translation-profile configuration mode. |
| **Example:** | |
| `Router(cfg-translation-profile)# exit` | |
| **Step 9**        |         |
| `ephone-dn tag` | Enters ephone-dn configuration mode to create an extension (ephone-dn) for a Cisco Unified IP phone line, an intercom line, a paging line, a voice-mail port, or a message-waiting indicator (MWI).  
  - `tag`—Unique sequence number that identifies this ephone-dn during configuration tasks. Range is from 1 to the maximum number of ephone-dns allowed on the router platform. Refer to CLI help for the maximum value for this argument. |
| **Example:** | |
| `Router(config)# ephone-dn 1` | |
| **Step 10**       |         |
| `translation-profile {incoming | outgoing} name` | Assigns a translation profile for incoming or outgoing call legs to or from Cisco Unified IP phones.  
  - `incoming`—Applies the translation profile to incoming calls.  
  - `outgoing`—Applies the translation profile to outgoing calls.  
  - `name`—The name of the translation profile. |
| **Example:** | |
| `Router(config-ephone-dn)# translation-profile outgoing name1` | |
| **Step 11**       |         |
| `exit` | Exits ephone-dn configuration mode. |
| **Example:** | |
| `Router(config-ephone-dn)# exit` | |
Examples

The following example shows the configuration where a translation profile called profile1 is created with two voice translation rules. Rule1 consists of associated calling numbers, and rule2 redirects called numbers. Ephone-dn 1 is configured with profile1.

```
voice translation-profile name1
  translate calling rule1
  translate redirect-called rule2

ephone-dn 1
  number 1001
  translation-profile incoming name1
```

Troubleshooting Voice Translation Rules and Profiles

**Step 1** Use the `show voice translation-rule` command to display the translation rules, and the `show voice translation-profile` command to display translation profiles.

```
Router# show voice translation-rule 6
Translation-rule tag: 6
  Rule 1:
    Match pattern: 65088801..
    Replace pattern: 6508880101
    Match type: none  Replace type: none
    Match plan: none  Replace plan: none
```

**Step 2** Use the `test voice translation-rule` command to test your translation profiles. For more information about this command, go to http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123tcr/123tvr/vrht_t1.htm#wp1488921.

```
Router(config)# voice translation-rule 5
Router(cfg-translation-rule)# rule 1 /201/ /102/
Router(cfg-translation-rule)# exit
Router(config)# exit
Router# test voice translation-rule 5 2015550101
Matched with rule 5
  Original number:2015550101  Translated number:1025550101
  Original number type: none  Translated number type: none
  Original number plan: none  Translated number plan: none
```

Feature History for Voice Translation Rules and Profiles

<table>
<thead>
<tr>
<th>Cisco Unified CME Version</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.2</td>
<td>Support for translation rules and profiles was introduced.</td>
</tr>
</tbody>
</table>
Related Features

**Ephone-Dn Templates**
Translation rules and translation profiles can be added to ephone-dn templates that are applied to one or more ephone-dns. For more information, see the “Ephone-dn Templates” section on page 322.
Cisco Unified CME GUI Support

This module describes the Cisco Unified CME graphical user interface (GUI) and explains how to set it up for three different classes of user. It contains the following sections:

- Cisco Unified CME GUI Support Overview, page 123
- Setting Up Initial Access for the GUI Administrator, page 125
- Accessing the Cisco Unified CME GUI, page 128
- Setting Up GUI Access for Customer Administrators, page 129
- Setting Up GUI Access for Phone Users, page 134
- Verifying Cisco Unified CME GUI Configuration, page 135
- Examples, page 136
- Troubleshooting the Cisco Unified CME GUI, page 136
- Feature History for the Cisco Unified CME GUI, page 136

**Note**

Cisco Unified CME GUI Support Overview

**Note**
If you are downgrading or upgrading Cisco Unified CME and use the Cisco Unified CME GUI, you must downgrade or upgrade your GUI files. For more information, see the “Downloading Cisco Unified CME Software” section on page 48.

**Note**
For a summary of the functionality introduced in different releases, see the “Feature History for the Cisco Unified CME GUI” section on page 136.
The Cisco Unified CME GUI provides a web-based interface to manage most systemwide and phone-based features. In particular, the GUI facilitates the routine adds and changes associated with employee turnover, allowing these changes to be performed by nontechnical staff. The GUI provides three levels of access to support the following user classes:

- System administrator—Able to configure all systemwide and phone-based features. This person is familiar with Cisco IOS software and VoIP network configuration.
- Customer administrator—Able to perform routine phone adds and changes without having access to systemwide features. This person does not have to be trained in Cisco IOS software.
- Phone user—Able to program a small set of features on his or her own phone and search the Cisco Unified CME directory.

The Cisco Unified CME GUI uses HTTP to transfer information from the router to the PC of an administrator or phone user. The router must be configured as an HTTP server, and an initial system administrator username and password must be defined from the router command-line interface (CLI). Additional customer administrators and phone users can be added from the Cisco Unified CME router using CLI commands or from a PC using GUI screens.

Cisco Unified CME provides support for eXtensible Markup Language (XML) cascading style sheets (files with a .css suffix) that can be used to customize the browser GUI display.

The GUI supports authentication, authorization, and accounting (AAA) authentication for system administrators through a remote server when this capability is enabled with the `ip http authentication` command. If authentication through the server fails, the local router is searched.

The sequence of tasks to set up the Cisco Unified CME GUI is as follows:

1. **Setting Up Initial Access for the GUI Administrator**—Define the HTTP server on the Cisco Unified CME router and create an account for the system administrator to log on to the GUI.
2. **Accessing the Cisco Unified CME GUI**—Log on to the GUI as the system administrator to verify its installation.
3. **Setting Up GUI Access for Customer Administrators**—Optionally create accounts for customer administrators to use to log on to the GUI. You can create additional accounts from the GUI itself or with router CLI.
4. **Setting Up GUI Access for Phone Users**—Optionally create accounts for phone users to use to log on to the GUI. You can create additional accounts from the GUI itself or with router CLI.

### Prerequisites

Files required for the operation of the GUI must have been be copied into flash memory on the router. For information about files, see the “Downloading Cisco Unified CME Software” section on page 48.

Note Cisco Unified CME GUI files are version-specific; GUI files for one version of Cisco Unified CME are not compatible with any other version of Cisco Unified CME. When Cisco Unified CME is downgraded or upgraded, the GUI files for the old version must be overwritten with GUI files that match the Cisco Unified CME version that is being installed.
Restrictions

- The web browser that you use to access the GUI must be Microsoft Internet Explorer Version 5.5 or a later version. No other type of browser can be used to access the GUI.
- If you use an XML configuration file to create a customer administrator login, the size of that XML file must be 4000 bytes or smaller.
- The password of the system administrator cannot be changed through the GUI. Only the password of a customer administrator or a phone user can be changed through the GUI.
- If more than 100 phones are configured, choosing to display all phones will result in a long delay before results are shown.

Setting Up Initial Access for the GUI Administrator

To set up GUI access for the Cisco Unified CME system administrator, complete the following tasks:
- Setting Up the HTTP Server, page 125 (required)
- Setting Up GUI Access for the System Administrator, page 126 (required)

Setting Up the HTTP Server

By default the HTTP server on a router is disabled. This task enables the HTTP server, specifies the path to files that are used for the GUI, and specifies a method of user authentication for security.

Use of the `ip http authentication` command is critical to prevent unauthorized users from accessing the Cisco Unified CME router. The default if this command is not used is that only the `enable` password for the router is needed to authenticate user access to the GUI. Use of only the `enable` password for authentication is strongly discouraged. Instead, Cisco recommends use of the local or TACACS authentication options, configured as part of a global AAA framework and specified by the `ip http authentication` command. By explicitly using the `ip http authentication` command, you designate alternative authentication methods, such as by a local login account or by the method that is specified in the AAA configuration on the Cisco Unified CME router. If you select the AAA authentication method, you must also define an authentication method in your AAA configuration, using commands similar to the ones in this example but appropriate for your situation:

```
aaa new-model
aaa authentication login default group tacacs+ local
tacacs-server host 10.1.2.3
```


SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `ip http server`
4. `ip http path flash:`
5. `ip http authentication {aaa | enable | local | tacacs}`
DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable          | Enables privileged EXEC mode.  
| **Example:**              |         |
| Router> enable             |         |
| **Step 2** configure terminal | Enters global configuration mode.  
| **Example:**               |         |
| Router# configure terminal |         |
| **Step 3** ip http server | Enables the Cisco web browser user interface on the local Cisco Unified CME router.  
| **Example:**               |         |
| Router(config)# ip http server |         |
| **Step 4** ip http path flash: | Sets the base HTTP path for HTML files to flash memory on the router.  
| **Example:**               |         |
| Router(config)# ip http path flash: |         |
| **Step 5** ip http authentication {aaa | enable | local | tacacs} | Specifies method of authentication to use for the HTTP server. Default is the enable keyword.  
| **Example:**               |         |
| Router(config)# ip http authentication aaa |         |

Setting Up GUI Access for the System Administrator

This task defines an initial username and password for a system administrator to use to access the GUI and enables the GUI to be used to set the time and to add directory listings.

Once you have created this account, you can log in to the GUI and create additional login accounts using the GUI itself. Alternatively, you can continue to use router CLI to create additional accounts. Both methods are explained in the sections following this section.
### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `telephony-service`
4. `web admin system name username {password string | secret {0 | 5} string}`
5. `dn-webedit`
6. `time-webedit`
7. `exit`

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 <code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Enter your password if prompted.</td>
</tr>
<tr>
<td>Step 2 <code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Step 3 <code>telephony-service</code></td>
<td>Enters telephony-service configuration mode.</td>
</tr>
<tr>
<td>Step 4 `web admin system name username {password string</td>
<td>secret {0</td>
</tr>
<tr>
<td>Example:</td>
<td>Note: The <code>secret 5</code> keyword pair is used in the output of <code>show</code> commands when encrypted passwords are displayed. It indicates that the password that follows is encrypted.</td>
</tr>
</tbody>
</table>

#### Command or Action Purpose

- **Step 1 `enable`**
  - Enables privileged EXEC mode.
  - Example: `Router> enable`
  - Enter your password if prompted.

- **Step 2 `configure terminal`**
  - Enters global configuration mode.
  - Example: `Router# configure terminal`

- **Step 3 `telephony-service`**
  - Enters telephony-service configuration mode.
  - Example: `Router(config)# telephony-service`

- **Step 4 `web admin system name username {password string | secret {0 | 5} string}`**
  - Defines a username and password for a system administrator. The default username is Admin. There is no default password.
  - Example: `Router(config-telephony)# web admin system name pwa3 secret 0 wp78pw`
  - Note: The `secret 5` keyword pair is used in the output of `show` commands when encrypted passwords are displayed. It indicates that the password that follows is encrypted.
Accessing the Cisco Unified CME GUI

The Cisco Unified CME GUI requires use of Microsoft Internet Explorer (IE) Version 5.5 or a later release. No other type of browser can be used to access the GUI.

To access the Cisco Unified CME router through the web to make configuration changes, point your IE 5.5 browser (or a later version) to the following URL:

http://router_ipaddr/ccme.html

where router_ipaddr is the IP address of your Cisco Unified CME router. For example, if the IP address of your Cisco Unified CME router is 10.10.10.176, enter the following:

http://10.10.10.176/ccme.html

You are presented with a login screen. Enter your username and password.

The Cisco Unified CME system evaluates your privilege level and presents the appropriate screen. Note that users with Cisco IOS software privilege level 15 also have system-administrator-level privileges in the Cisco Unified CME GUI once they have been authenticated locally or remotely through AAA. The ip http authentication command that has been configured on the Cisco Unified CME router determines where authentication occurs.
After you have been logged in and have been authenticated, you see one of the following home screens, based on your user class:

- The system administrator home screen.
- The customer administrator sees a reduced version of the options available on the system administrator screen, according to the XML configuration file that the system administrator created.
- The phone user home screen.

After you log in successfully, online help is available from the Help menu.

**Setting Up GUI Access for Customer Administrators**

After creating a system administrator account for GUI access, you can create accounts for customer administrators so that they can log in to the GUI from their PCs. You can create these accounts using router CLI or by using the GUI itself. These procedures are explained in the following sections:

- Creating and Loading an XML Configuration File, page 129
- Defining a Customer Administrator, page 132

**Creating and Loading an XML Configuration File**

The XML configuration file specifies the characteristics and features that you want to make available to customer administrators and the characteristics and features that should be restricted. The file follows a template that conforms to the Cisco XML Document Type Definition (DTD), which is documented in *Cisco IP Phone Services Application Development Notes*. The template is named xml.template and is one of the Cisco Unified CME files that you download from the Cisco Software Center when you first set up a Cisco Unified CME system. The XML template is shown in the “XML Configuration File Template Example” section on page 130 and a sample XML file is shown in “XML Configuration File Example” section on page 131.

Edit and load the XML configuration file by using the following steps.

**SUMMARY STEPS**

1. Make a copy of the XML template and open it in any text editor.
2. Edit the XML template.
3. Copy the file to a TFTP or FTP server that can be accessed by the Cisco Unified CME router.
4. Copy your file to flash memory on the Cisco Unified CME router.
5. Load the XML file from router flash memory.

**DETAILED STEPS**

**Step 1**

Make a copy of the XML template that you downloaded from the Cisco Software Center (shown in the “XML Configuration File Template Example” section on page 130) and open it in any text editor. Give the file a name that is meaningful to you and that uses “xml” as its suffix. For example, you could name the file “custadm.xml.”
**Step 2** Edit the XML template. Within the template, each line that starts with a title enclosed in angle brackets describes an XML object and matches an entity name in the CME GUI. For example, “<AddExtension>” refers to the Add Extension capability, and “<Type>” refers to the Type field on the Add Extension screen. For each object in the template, you have a choice of actions. Your choices appear within brackets; for example, “[Hide | Show]” indicates that you have a choice between whether this object is hidden or visible when a customer administrator logs into the GUI. Delete the action that you do not want and the vertical bar and brackets around the actions.

For example, to hide the Sequence Number field, change the following text in the template file:

```xml
<SequenceNumber> [Hide | Show] </SequenceNumber>
```

to the following text in your configuration file:

```xml
<SequenceNumber> Hide </SequenceNumber>
```

Edit every line in the template until you have changed each choice in brackets to a single action and you have removed the vertical bars and brackets. A sample XML file is shown in the “XML Configuration File Example” section on page 131.

**Step 3** Copy the file to a TFTP or FTP server that can be accessed by the Cisco Unified CME router.

**Step 4** Copy your file to flash memory on the Cisco Unified CME router.

Router# `copy tftp flash`

**Step 5** Load the XML file from router flash memory.

Router(config)# `telephony-service`
Router(config-telephony)# `web customize load filename`
Router(config-telephony)# `exit`

---

**XML Configuration File Template Example**

```xml
<Presentation>
  <MainMenu>
    <!--[!-- Take Higher Precedence over CLI "dn-web-edit" -->]
    <AddExtension> [Hide | Show] </AddExtension>
    <DeleteExtension> [Hide | Show] </DeleteExtension>
    <AddPhone> [Hide | Show] </AddPhone>
    <DeletePhone> [Hide | Show] </DeletePhone>
  </MainMenu>
  <Extension>
    <!--[!-- Control both view and change, and possible add or delete -->]
    <SequenceNumber> [Hide | Show] </SequenceNumber>
    <Type> [Hide | Show] </Type>
    <Huntstop> [Hide | Show] </Huntstop>
    <Preference> [Hide | Show] </Preference>
    <HoldAlert> [Hide | Show] </HoldAlert>
    <TranslationRules> [Hide | Show] </TranslationRules>
    <Paging> [Hide | Show] </Paging>
    <Intercom> [Hide | Show] </Intercom>
    <MWI> [Hide | Show] </MWI>
    <MoH> [Hide | Show] </MoH>
    <LBDN> [Hide | Show] </LBDN>
    <DualLine> [Hide | Show] </DualLine>
    <Reg> [Hide | Show] </Reg>
    <PGroup> [Hide | Show] </PGroup>
  </Extension>
</Presentation>
```
<Phone>
   <!-- control both view and change, and possible add and delete --->
   <SequenceNumber> [Hide | Show] </SequenceNumber>
</Phone>

<System>
   <!-- Control View Only -->
   <PhoneURL> [Hide | Show] </PhoneURL>
   <PhoneLoad> [Hide | Show] </PhoneLoad>
   <CallHistory> [Hide | Show] </CallHistory>
   <MWIServer> [Hide | Show] </MWIServer>
   <!-- Control Either View and Change or Change Only -->
   <TransferPattern attr=[Both | Change]> [Hide | Show] </TransferPattern>
   <VoiceMailNumber attr=[Both | Change]> [Hide | Show] </VoiceMailNumber>
   <MaxNumberPhone attr=[Both | Change]> [Hide | Show] </MaxNumberPhone>
   <DialplanPattern attr=[Both | Change]> [Hide | Show] </DialplanPattern>
   <SecDialTone attr=[Both | Change]> [Hide | Show] </SecDialTone>
   <Timeouts attr=[Both | Change]> [Hide | Show] </Timeouts>
   <CIDBlock attr=[Both | Change]> [Hide | Show] </CIDBlock>
   <HuntGroup attr=[Both | Change]> [Hide | Show] </HuntGroup>
   <NightSerBell attr=[Both | Change]> [Hide | Show] </NightSerBell>
   <!-- Control Change Only -->
   <!-- Take Higher Precedence over CLI "time-web-edit" -->
   <Time> [Hide | Show] </Time>
</System>

<Function>
   <AddLineToPhone> [No | Yes] </AddLineToPhone>
   <DeleteLineFromPhone> [No | Yes] </DeleteLineFromPhone>
   <NewDnDpCheck> [No | Yes] </NewDnDpCheck>
   <MaxLinePerPhone> [1-6] </MaxLinePerPhone>
</Function>

</Presentation>

XML Configuration File Example

sample.xml
<Presentation>
   <MainMenu>
      <AddExtension> Hide </AddExtension>
      <DeleteExtension> Hide </DeleteExtension>
      <AddPhone> Hide </AddPhone>
      <DeletePhone> Hide </DeletePhone>
   </MainMenu>

   <Extension>
      <SequenceNumber> Hide </SequenceNumber>
      <Type> Hide </Type>
      <Huntstop> Hide </Huntstop>
      <Preference> Hide </Preference>
      <HoldAlert> Hide </HoldAlert>
      <TranslationRule> Hide </TranslationRule>
      <Paging> Show </Paging>
      <Intercom> Hide </Intercom>
      <MWI> Hide </MWI>
      <MoH> Hide </MoH>
      <LBDN> Hide </LBDN>
      <DualLine> Hide </DualLine>
      <Reg> Hide </Reg>
      <PGroup> Show </PGroup>
   </Extension>

</Presentation>
Defining a Customer Administrator

You can define a login account for a customer administrator in either of the following two ways:

- Method 1: Using the Cisco Unified CME GUI to Define a Customer Administrator, page 132
- Method 2: Using the Cisco IOS CLI to Define a Customer Administrator, page 133

Method 1: Using the Cisco Unified CME GUI to Define a Customer Administrator

This method allows the system administrator to use the GUI itself to create a customer administrator login account for the GUI.

SUMMARY STEPS

1. From the Configure System Parameters menu, choose Administrator’s Login Account.
2. Complete the Admin User Name (username), Admin User Type (Customer), and New Password fields.
3. Click Change.
**DETAILED STEPS**

**Step 1**  
From the Configure System Parameters menu, choose **Administrator’s Login Account**.

**Step 2**  
Complete the Admin User Name (username), Admin User Type (Customer), and New Password fields for the user that you are defining as a customer administrator. Type the password again to confirm it.

**Step 3**  
Click **Change** for your changes to become effective.

**Method 2: Using the Cisco IOS CLI to Define a Customer Administrator**

This method allows the system administrator to create a customer administrator account for the Cisco Unified CME GUI by using the Cisco IOS CLI.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. telephony-service
4. `web admin customer name username password string`
5. exit

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
• Enter your password if prompted. |
| **Step 2** configure terminal | Enters global configuration mode. |
| **Step 3** telephony-service | Enters telephony-service configuration mode. |

**Example:**

- `Router> enable`
- `Router# configure terminal`
- `Router(config)# telephony-service`
Setting Up GUI Access for Phone Users

After creating a system administrator account for GUI access, you can create accounts for individual phone users so that they can log in to the GUI from their PCs. You can create these accounts using router CLI or by using the GUI itself. These procedures are explained in the following sections:

You can enable GUI access for a phone user in either of the following two ways:

- Method 1: Using the Cisco Unified CME GUI to Define a GUI Account for a Phone User, page 134
- Method 2: Using the Cisco IOS CLI to Define a GUI Account for a Phone User, page 135

Method 1: Using the Cisco Unified CME GUI to Define a GUI Account for a Phone User

This method uses the Cisco Unified CME GUI itself to create a GUI login account for a phone user.

**SUMMARY STEPS**

1. From the Configure Phones menu, choose Add Phone or Change Phone.
2. Enter a username and password in the Login Account area of the screen.
3. Click Change.

**DETAILED STEPS**

**Step 1**
From the Configure Phones menu, choose Add Phone to add GUI access for a user with a new phone or Change Phone to add GUI access for a user with an existing phone. You see the Add Phone screen or the Change Phone screen.

**Step 2**
Enter a username and password in the Login Account area of the screen. If you are adding a new phone, complete the other fields as appropriate.

**Step 3**
Click Change for your edits to become effective.

---

**Command or Action** | **Purpose**
--- | ---
web admin customer name username password string | Defines a username and password for a customer administrator. The default username is Customer. There is no default password.

*Example:*

Router(config-telephony)# web admin customer name user44 password pw10293847

**Step 5**
ext

*Example:*

Router(config-telephony)# exit

Exits telephony-service configuration mode.
Method 2: Using the Cisco IOS CLI to Define a GUI Account for a Phone User

This method uses the Cisco IOS CLI to create a Cisco Unified CME GUI login account for a phone user.

SUMMARY STEPS

1. enable
2. configure terminal
3. ephone phone-tag
4. username username password password
5. exit

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Enter your password if prompted.</td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Step 3 ephone tag</td>
<td>Enters ephone configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Step 4 username username password password</td>
<td>Assigns a phone user login account name and password.</td>
</tr>
<tr>
<td>Example:</td>
<td>This allows individual phone users to log in to the Cisco Unified CME router through a web interface to change a limited number of personal settings.</td>
</tr>
<tr>
<td>Step 5 exit</td>
<td>Exits ephone configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>

Verifying Cisco Unified CME GUI Configuration

Step 1 Use the show running-config command to display telephony-service and ephone settings for Cisco Unified CME GUI accounts.
Examples

The following example sets up the HTTP server and creates a system administrator account for pwa3, a customer administrator account for user44, and a user account for prx.

```
ip http server
ip http path flash:
ip http authentication aaa
telephony-service
  web admin system name pwa3 secret 0 wp78pw
  web admin customer name user44 password pw10293847
dn-webedit
time-webedit
ephone 25
  username prx password pk59wq
```

Troubleshooting the Cisco Unified CME GUI

If you are having trouble starting the Cisco Unified CME GUI, try the following actions:

---

**Step 1** Make sure you are using Microsoft Internet Explorer (IE) Version 5.5 or a later release. No other type of browser can be used to access the GUI.

**Step 2** Clear your browser cache or history.

**Step 3** Make sure that you have in router flash memory the correct version of the GUI files for the version of Cisco Unified CME that you have. Compare the filenames in flash memory with the list in the Cisco Unified CME software archive that you downloaded. Compare the sizes of files in flash memory with the sizes of the files in the tar archive called cme-3.2.0-gui.tar (or a later version of the file) to be sure that you have the most recent files installed in flash memory. The latest version can be downloaded from the Cisco Unified CME Software Download website at [http://www.cisco.com/cgi-bin/tablebuild.pl/ip-iostsp](http://www.cisco.com/cgi-bin/tablebuild.pl/ip-iostsp).

---

Feature History for the Cisco Unified CME GUI

<table>
<thead>
<tr>
<th>Cisco Unified CME Version</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.0</td>
<td>The Cisco Unified CME GUI was introduced.</td>
</tr>
</tbody>
</table>
Phone Support

Cisco Unified CME provides call control for many kinds of phones. This chapter contains the following sections:

- Phone Support Overview, page 137
- Analog Phones, page 138
- Cisco IP Communicator, page 140
- Teleworker Remote Phones, page 143

**Note**

Phone Support Overview

The types of phones and the phone firmware versions that Cisco Unified CME supports are listed in the Cisco Unified CME specifications document for each release. To find the Cisco Unified CME specifications for your particular release, see the *Cisco CME Documentation Roadmap*.

Most of the phones used with Cisco Unified CME are IP phones. Basic phone configuration for IP phones is discussed in the “Installing Cisco Unified CME” section on page 43. However, there are some special cases, which are described in this chapter and summarized in Table 20.

<table>
<thead>
<tr>
<th><strong>Table 20</strong></th>
<th><strong>Phone Support Summary</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Feature</td>
<td>Description</td>
</tr>
<tr>
<td>Analog Phones</td>
<td>System supports connection of phones or fax machines in SCCP or H.323 mode.</td>
</tr>
</tbody>
</table>
Analog Phones Overview

Cisco Unified CME supports analog phones using Cisco Analog Telephone Adapters (ATA) or FXS ports in SCCP mode or H.323 mode, and supports fax machines on ATA or FXS ports in H.323 mode. The FXS ports used for analog phones or fax can be on the Cisco Unified CME router or on a Cisco VG 224 voice gateway. This section provides information on the following topics:

- FXS Ports in SCCP Mode, page 138
- FXS Ports in H.323 Mode, page 139
- Restrictions for Analog Phones, page 139

FXS Ports in SCCP Mode

FXS ports on Cisco VG 224 Analog Phone Gateways can be configured for SCCP supplementary features in Cisco CME 3.2.1 and later versions. The Cisco VG 224 must be running Cisco IOS Release 12.4(2)T or a later release. For information about using SCCP supplementary features on analog FXS ports on a Cisco VG 224 under the control of a Cisco Unified CME system, see SCCP Controlled Analog (FXS) Ports with Supplementary Features in Cisco IOS Gateways and the Cisco VG 224 Analog Phone Gateway data sheet.
FXS Ports in H.323 Mode

FXS ports on platforms that cannot enable SCCP supplementary features can use H.323 mode to support
call waiting, caller ID, hookflash transfer, modem pass-through, fax (T.38, Cisco fax relay, and
pass-through), and PLAR. These features are provisioned as Cisco IOS voice features and not as
Cisco Unified CME features. Note that when using Cisco Unified CME, you can configure FXS ports in
H.323 mode for call waiting or hookflash transfer, but not both at the same time.

The following links provide details on configuring analog phone features for FXS ports in H.323 mode:

- “Configuring Analog Voice Ports” section in Voice Ports Configuration
- “Caller ID” section of the Cisco IOS Voice Configuration Library
- “Modem Support for VoIP” section of the Cisco IOS Voice Configuration Library
- Cisco IOS Fax and Modem Services over IP Application Guide

Restrictions for Analog Phones

- Support for Skinny Client Control Protocol (SCCP) supplementary features on analog FXS ports is
  as follows:
  - FXS ports on Cisco VG 224 Analog Phone Gateways require Cisco CME 3.2.1 or a later
    version. The Cisco VG 224 must be running Cisco IOS Release 12.4(2)T or a later release.
  - FXS ports on Cisco VG 248 Analog Phone Gateways are not supported by Cisco Unified CME.
- Cisco Unified CME features such as call forward and call park are not available for analog phones
  connected to FXS ports in H.323 mode. In order to support these features, SCCP supplementary
  features must be enabled on the FXS ports.
- For a Cisco ATA that is registered to a Cisco Unified CME system to participate in fax calls, it must
  have its ConnectMode parameter set to use the same RTP payload type as the Cisco voice gateway
  that is performing the fax pass-through. Cisco voice gateways currently use standard payload
  type 0/8, which is selected on Cisco ATAs by setting bit 2 of the ConnectMode parameter to 1. For
  more information, see the “Parameters and Defaults” chapter in the Cisco ATA 186 and

Feature History for Analog Phones

<table>
<thead>
<tr>
<th>Cisco Unified CME Version</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>Support was introduced for analog phones in H.323 mode using FXS ports.</td>
</tr>
<tr>
<td>3.0</td>
<td>Support was introduced for Cisco ATA 186 and Cisco ATA 188.</td>
</tr>
<tr>
<td>3.2.1 and Cisco IOS Release 12.4(2)T</td>
<td>Support was introduced for analog phones with SCCP supplementary features using FXS ports on a Cisco VG 224 voice gateway.</td>
</tr>
</tbody>
</table>
| 4.0                       | - Support was introduced for fax pass-through mode using SCCP and a Cisco VG 224 voice gateway or Cisco ATA.  
  - Support was introduced for analog phones with SCCP supplementary features using FXS ports on Cisco Integrated Services Routers. |
Related Features

SCCP Analog Phones Using Ports on Cisco VG 224
This feature provides Cisco IOS software support to enable Skinny Client Control Protocol (SCCP) supplementary features on analog FXS ports on a Cisco VG 224 voice gateway under the control of a Cisco Unified CME system. For more information, see SCCP Controlled Analog (FXS) Ports with Supplementary Features in Cisco IOS Gateways.

Feature Access Codes (FAC)
This feature provides phone user dialing codes to access SCCP supplementary features. For more information, see the “Feature Access Codes” section on page 325.

Fax Services
Fax services are described in the Cisco IOS Fax and Modem Services over IP Application Guide.
Fax services using Cisco ATA are described in the “Configuring and Debugging Fax Services” chapter of the Cisco ATA 186 and Cisco ATA 188 Analog Telephone Adaptor Administrator’s Guide for SCCP version 3.0. Also see the restriction in the “Restrictions for Analog Phones” section on page 139.

Cisco IP Communicator
Cisco IP Communicator is a software-based application that delivers enhanced telephony support on personal computers. This section includes the following topics:

- Cisco IP Communicator Overview, page 140
- Configuring Cisco IP Communicator, page 141
- Verifying Cisco IP Communicator, page 141
- Troubleshooting Cisco IP Communicator, page 142
- Feature History for Cisco IP Communicator, page 142
- Related Features, page 142

Cisco IP Communicator Overview
Cisco IP Communicator is a software-based application that delivers enhanced telephony support on personal computers. Cisco IP Communicator appears on a user’s computer monitor as a graphical, display-based IP phone with a color screen, a key pad, feature buttons, and soft keys.
For information about operation, see the Cisco IP Communicator user documentation and online help.

Prerequisites
You should have the following available before you begin this task:

- IP address of the Cisco Unified CME TFTP server
- (Optional) Headsets with microphones for users
Configuring Cisco IP Communicator

SUMMARY STEPS

1. Download the latest version of the Cisco IP Communicator software and install it on your PC.
2. (Optional) Attach a headset with microphone to your PC.
3. Start the Cisco IP Communicator software application.
4. Define the IP address of the Cisco Unified CME TFTP server.
5. Wait for the Cisco IP Communicator application to connect to the Cisco Unified CME system and register itself.
6. Perform the final configuration of line buttons and extension numbers for the Cisco IP Communicator from the Cisco Unified CME router.

DETAILED STEPS

Step 1  Download the latest version of the Cisco IP Communicator software and install it on your PC.
Cisco Unified CME 4.0 and later versions require Cisco IP Communicator 2.0 or a later version.

Step 2  (Optional) Attach a headset with microphone to your PC.

Step 3  Start the Cisco IP Communicator software application.

Step 4  Define the IP address of the Cisco Unified CME TFTP server.
   a. Open the Network > User Preferences window.
   b. Enter the IP address of the Cisco Unified CME TFTP server.

Step 5  Wait for the Cisco IP Communicator application to connect to the Cisco Unified CME system and register itself.

Step 6  Perform the final configuration of line buttons and extension numbers for the Cisco IP Communicator from the Cisco Unified CME router.
Use the normal phone provisioning commands described in the “Task 6: Provisioning Phones” section on page 70. In the type command, use the CIPC keyword to identify this phone as a Cisco IP Communicator.

Verifying Cisco IP Communicator

Step 1  Use the show running-config command to display ephone-dn and ephone information associated with this phone.

Step 2  After Cisco IP Communicator registers with Cisco Unified CME, it displays the phone extensions and soft keys in its configuration. Verify that these are correct.

Step 3  Make a local call from the phone and ask someone to call you. Verify that you have a two-way voice path.
Troubleshooting Cisco IP Communicator

Step 1 Use the `debug ephone detail` command to diagnose problems with calls. For more information, see the *Cisco IOS Debug Command Reference*.

Feature History for Cisco IP Communicator

<table>
<thead>
<tr>
<th>Cisco Unified CME Version</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.0</td>
<td>Support for Cisco IP Communicator was introduced.</td>
</tr>
</tbody>
</table>

Related Features

**Basic Phone Configuration**

The ephone-dn and ephone configuration for a Cisco IP Communicator is the same as that for a physical IP phone. For more information, see the “Installing Cisco Unified CME” section on page 43.

SIP Phones

Cisco Unified CME provides station-side RFC3261 standard-based support for SIP phones. This section includes the following topics:

- SIP Phones Overview, page 142
- Feature History for SIP Phones, page 143

SIP Phones Overview

Cisco Unified CME acts as the primary SIP registrar for SIP phones. The following call combinations are supported:

- Direct calls between local SIP phones
- Incoming and outgoing calling between SIP phones
- Incoming and outgoing calling between a SIP phone and a SCCP phone
- SIP phone to WAN VoIP using SIP protocol

For more information and configuration instructions, see the *Cisco CallManager Express 3.4 Configuration Guide*.
**Feature History for SIP Phones**

<table>
<thead>
<tr>
<th>Cisco Unified CME Version</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.4</td>
<td>Support for SIP phones was introduced.</td>
</tr>
</tbody>
</table>

**Teleworker Remote Phones**

This feature allows IP phones or instances of Cisco IP Communicator to be connected to a Cisco Unified CME system over a wide area network (WAN). This section includes the following topics:

- Teleworker Remote Phones Overview, page 143
- Configuring a Teleworker Remote Phone, page 146
- Verifying Teleworker Remote Phones, page 147
- Examples, page 147
- Feature History for Teleworker Remote Phones, page 147
- Related Features, page 148

**Teleworker Remote Phones Overview**

Note: Cisco Unified CME does not currently support Emergency 911 (E911) calls from remote IP phones. For more information, see the “Restrictions” section on page 145.

IP phones or instances of Cisco IP Communicator can be connected to a Cisco Unified CME system over a WAN to support teleworkers who have offices that are remote from the Cisco Unified CME router. The maximum number of remote phones that can be supported is determined by the available bandwidth.

IP addressing is the most critical aspect of remote teleworker phone design. The following two scenarios represent the most common designs, with the second one being the most common among small and medium businesses:

- Remote site IP phones and the hub Cisco Unified CME router use globally routable IP addresses.
- Remote site IP phones use NAT with non-routable private IP addresses and the hub Cisco Unified CME router uses a globally routable address (see Figure 14). This scenario results in one-way audio unless you use one of the following workarounds:
  - Configure static NAT mapping on the remote site router (such as a Cisco 831 Ethernet Broadband Router) to convert between a private address and a globally routable address. This solution uses fewer Cisco Unified CME resources, but voice is unencrypted across the WAN.
  - Configure an IPsec VPN tunnel between the remote site router (such as a Cisco 831) and the Cisco Unified CME router. This solution requires an Advanced IP Services or higher image on the Cisco Unified CME router if this router is used to terminate the VPN tunnel. Voice will be encrypted across the WAN. This method will also work with the Cisco VPN client on a PC to support Cisco IP Communicator.
To facilitate remote phone connections over a WAN, the following parameters can be specified. They are optional, but recommended.

- **Media Packet Destination, page 144**
- **Codec (G.711 or G.729r8), page 144**

**Media Packet Destination**

The `mtp` command is used to ensure that media packets (Real-Time Transport Protocol or RTP packets) from remote phones will always transit through the Cisco Unified CME router. Without this command, a phone that is connected in a call with another phone in the same Cisco Unified CME system sends its media packets directly to the other phone, without the packets going through the Cisco Unified CME router. The `mtp` command forces the media packets to be sourced from the Cisco Unified CME router.

The reason you want to use the `mtp` command is because phones that are connected over a WAN may have their media packets obstructed by a firewall (see Figure 14). When the `mtp` command is used to instruct a phone to always send its media packets to the Cisco Unified CME router, the router acts as a media termination point (MTP) or proxy and forwards the packets to the destination phone. If a firewall is present, it can be easily configured to pass the RTP packets because the router uses a specified UDP port for media packets. In this way, RTP packets from remote IP phones can be delivered to IP phones on the same system even though they must pass through a firewall.

The default is that the MTP function is not enabled, so you must explicitly use the `mtp` command for each remote phone that you want to send media packets to the Cisco Unified CME router.

One factor to consider when deciding to use the `mtp` command is whether you are using multicast music on hold (MOH) in your Cisco Unified CME system. Multicast packets generally cannot be forwarded to phones that are reached over a WAN. The multicast MOH feature checks to see if the `mtp` command has been configured for a phone and if it has been, MOH is not sent to that phone. If you have a WAN configuration that can forward multicast packets and you can allow RTP packets through your firewall, you can decide not to use the `mtp` command.

**Codec (G.711 or G.729r8)**

You can use the `codec` command to select the G.729r8 codec to help save network bandwidth for a remote IP phone. The default codec if this command is not used is G.711 mu-law. When you use the `codec` command without the `dspfarm-assist` keyword, the use of the G.729 codec is preserved only for calls between two phones on the Cisco Unified CME router (such as between an IP phone and another IP phone or between an IP phone and an FXS analog phone). The command has no effect on a call directed through a VoIP dial peer unless the `dspfarm-assist` keyword is also used.

When a Cisco Unified CME conference is initiated, all phones in the conference switch to G.711 mu-law, which may not be desirable for remote phones. To allow a phone to retain its G.729r8 codec setting even when being joined to a conference, you can use the `dspfarm-assist` keyword with the `codec` command. The `dspfarm-assist` keyword specifies that this phone’s calls should use the resources of a configured DSP farm for transcoding. For example, there are two remote phones (A and B) and a local
phone (C) that initiates a conference with them. Both A and B are configured to use the G.729r8 codec with the assistance of the DSP-farm transcoder. In the conference, the call leg from C to the conference uses the G.711 mu-law codec, and the call legs from A and B to the Cisco Unified CME router use the G.729r8 codec.

You should consider your options carefully when deciding to use the `dpfarm-assist` keyword with the `codec` command. The benefit is that it allows calls to use the G.729r8 codec on the call leg between the IP phone and the Cisco Unified CME router, which saves network bandwidth. The disadvantage is that for situations requiring G.711 codecs, such as conferencing and Cisco Unity Express, DSP resources that are possibly scarce will be used to transcode the call, and delay will be introduced while voice is shuttled to and from the DSP. In addition, the overuse of this feature can mask configuration errors in the codec selection mechanisms involving dial peers and codec lists.

Therefore, it is recommended that the `dpfarm-assist` keyword be used sparingly and only when absolutely required for bandwidth savings or when you know the phone will be participating very little, if at all, in calls that require a G.711 codec.

If the `dpfarm-assist` keyword has been configured for a phone and a DSP resource is not available when needed for transcoding, a phone registered to the local Cisco Unified CME router will use G.711 instead of G.729r8. This is not true for non-SCCP call legs; if no DSP resource is available for the transcoding required for a conference, for example, the conference will not be created.

For more information about DSP farms, see the “Transcoding Support” section on page 199.

**Prerequisites**

- The WAN link supporting one or more teleworker remote phones should be configured with a Call Admission Control (CAC) or Resource Reservation Protocol (RSVP) solution to prevent the oversubscription of bandwidth, which can degrade the quality of all voice calls.
- If DSP farms are going to be used for transcoding, you must configure them separately. See the “Transcoding Support” section on page 199.

**Restrictions**

- Because Cisco Unified CME is not designed for centralized call processing, teleworker remote phones are supported only for fixed teleworker applications, such as working from a home office.
- Cisco Unified CME does not support Call Admission Control (CAC) for remote SCCP phones, so voice quality can degrade if a WAN link is oversubscribed. High-bandwidth data applications used over a WAN can cause degradation of voice quality for remote IP phones.
- Cisco Unified CME does not currently support Emergency 911 (E911) calls from remote IP phones. Teleworkers using remote phones connected to Cisco Unified CME over a WAN should be advised not to use these phones for E911 emergency services because the local public safety answering point (PSAP) will not be able to obtain valid calling-party information from them.

It is highly recommended that you make all remote phone users aware of this issue. One way is to place a sticker on all teleworker remote phones that reminds users not to place 911 emergency calls on remote IP phones. Remote workers should place any emergency calls through locally configured hotel, office, or home phones (normal land-line phones) whenever possible. Inform remote workers that if they must use remote IP phones for emergency calls, they should be prepared to provide specific location information to the answering PSAP personnel, including street address, city, state, and country.
Configuring a Teleworker Remote Phone

SUMMARY STEPS

1. enable
2. configure terminal
3. ephone phone-tag
4. mtp
5. codec {g711ulaw | g729r8 [dspfarm-assist]}
6. exit

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> ephone phone-tag</td>
<td>Enters ephone configuration mode.</td>
</tr>
<tr>
<td>Example: Router(config)# ephone 36</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> mtp</td>
<td>Sends media packets to the Cisco Unified CME router.</td>
</tr>
<tr>
<td>Example: Router(config-ephone)# mtp</td>
<td></td>
</tr>
</tbody>
</table>
Verifying Teleworker Remote Phones

**Step 1**

Use the `show running-config` command or the `show telephony-service ephone` command to verify parameter settings for remote ephones.

**Examples**

The following example shows the configuration for ephone 270, a teleworker remote phone with its codec set to G.729r8. The `dspfarm-assist` keyword is used to ensure that calls from this phone will use DSP resources to maintain the G.729r8 codec even when calls would normally be switched to a G.711 codec.

```plaintext
ephone 270
button 1:36
mtp
codec g729r8 dspfarm-assist
description teleworker remote phone
```

**Feature History for Teleworker Remote Phones**

<table>
<thead>
<tr>
<th>Cisco Unified CME Version</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.0</td>
<td>Support for teleworker remote phones was introduced.</td>
</tr>
</tbody>
</table>
Related Features

Ephone Templates
This feature can also be configured using an ephone template. For configuration instructions, see the “Ephone Templates” section on page 318.

DSP Farms
For information on configuring DSP farms, see the “Transcoding Support” section on page 199.

Basic Phone Configuration
Ephone-dn and ephone configuration are the same for remote phones as for local phones. For more information, see the “Task 6: Provisioning Phones” section on page 70 in the “Installing Cisco Unified CME” chapter.
Phone Authentication

Cisco Unified CME phone authentication is a security infrastructure for providing secure Skinny Client Control Protocol (SCCP) signaling between Cisco Unified CallManager Express (Cisco Unified CME) and IP phones. This chapter contains the following sections:

- Phone Authentication Overview, page 149
- Configuring Phone Authentication, page 156
- Examples, page 192
- Feature History for Phone Authentication, page 196
- Related Features, page 196
- Glossary, page 196


Phone Authentication Overview

For a summary of the functionality introduced in different releases, see the “Feature History for Phone Authentication” section on page 196.

The goal of Cisco Unified CME phone authentication is to create a secure environment for an IP telephony system that is based on Cisco Unified CME. Phone authentication addresses the following security needs:

- Establishing the identity of each endpoint in the system
- Authenticating devices
- Providing signaling-session privacy
- Providing protection for configuration files

Cisco Unified CME phone authentication implements authentication and encryption in the Cisco Unified CME system to prevent identity theft of the phone or Cisco Unified CME system, data tampering, and call-signaling tampering or media-stream tampering. To prevent these threats, the
Cisco Unified IP telephony network establishes and maintains authenticated communication streams, digitally signs files before they are transferred to phones, and encrypts call signaling between Cisco Unified IP Phones.

Cisco Unified CME phone authentication provides the following types of authentication to enable secure communication:

- **Phone authentication**—This process occurs between the Cisco Unified CME router and a supported device when each entity accepts the certificate of the other entity; only then does a secure connection between the entities occur. Phone authentication relies on the creation of a Certificate Trust List (CTL) file, which is a list of known, trusted certificates and tokens. Phones communicate with Cisco Unified CME using a secure transport-layer-session (TLS) connection, which requires that the following criteria must be met:
  - A certificate must exist on the phone.
  - A phone configuration file must exist on the phone, and the Cisco Unified CME entry and certificate must exist in the file.
- **The phone must be configured for authentication or encryption.**
- **File authentication**—This process validates digitally signed files that a phone downloads from a Trivial File Transfer Protocol (TFTP) server—for example, configuration files, ring list files, locale files, and CTL files. When the phone receives these types of files from the TFTP server, the phone validates the file signatures to verify that file tampering did not occur after the files were created.
- **Signaling authentication**—This process, also known as signaling integrity, uses the TLS protocol to validate that signaling packets have not been tampered with during transmission. Signaling authentication relies on the creation of the CTL file.

### Public Key Infrastructure

Cisco Unified CME phone authentication uses the public-key-infrastructure (PKI) capabilities in Cisco IOS software for certificate-based authentication of IP phones. PKI provides customers with a scalable, secure mechanism for distributing, managing, and revoking encryption and identity information in a secured data network. Every entity (a person or a device) participating in the secured communication is enrolled in the PKI using a process in which the entity generates a Rivest-Shamir-Adleman (RSA) key pair (one private key and one public key) and has its identity validated by a trusted entity (also known as a certification authority [CA] or trustpoint).

After each entity enrolls in a PKI, every peer (also known as an end host) in a PKI is granted a digital certificate that has been issued by a CA.

When peers must negotiate a secured communication session, they exchange digital certificates. Based on the information in the certificate, a peer can validate the identity of another peer and establish an encrypted session with the public keys contained in the certificate.

For more information about PKI, see the “Implementing and Managing a PKI” section of the *Cisco IOS Security Configuration Guide.*
How PKI Works with Cisco Unified CME

A number of components work together to ensure secure communications in a Cisco Unified CME system. Table 21 defines the components and Figure 15 on page 154 shows them in a Cisco Unified CME phone authentication environment. Following the figure is a high-level review of the phone-authentication process and a list of the configuration tasks that a system administrator needs to perform to enable the phone-authentication components.

Table 21  Cisco Unified CME Phone Authentication Components

<table>
<thead>
<tr>
<th>Component</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>certificate</td>
<td>An electronic document that binds a user's or device's name to its public key. Certificates are commonly used to validate digital signatures. Certificates are needed for authentication during secure communication. An entity obtains a certificate by enrolling with the CA.</td>
</tr>
<tr>
<td>signature</td>
<td>An assurance from an entity that the transaction it accompanies is authentic. The entity's private key is used to sign transactions and the corresponding public key is used for decryption.</td>
</tr>
<tr>
<td>RSA key pair</td>
<td>RSA is a public key cryptographic system developed by Ron Rivest, Adi Shamir, and Leonard Adleman.</td>
</tr>
<tr>
<td></td>
<td>An RSA key pair consists of a public key and a private key. The public key is included in a certificate so that peers can use it to encrypt data that is sent to the router. The private key is kept on the router and used both to decrypt the data sent by peers and to digitally sign transactions when negotiating with peers.</td>
</tr>
<tr>
<td></td>
<td>You can configure multiple RSA key pairs to match policy requirements, such as key length, key lifetime, and type of keys, for different certificate authorities or for different certificates.</td>
</tr>
<tr>
<td>certificate server trustpoint</td>
<td>A certificate server generates and issues certificates upon receipt of legitimate requests. A trustpoint with the same name as the certificate server stores the certificates. Each trustpoint has one certificate plus a copy of the CA certificate.</td>
</tr>
<tr>
<td>certification authority (CA)</td>
<td>The ultimate certificate server or root certificate server. It is responsible for managing certificate requests and issuing certificates to participating network devices. This service provides centralized key management for participating devices and is explicitly trusted by the receiver to validate identities and to create digital certificates. The CA can be a Cisco IOS CA on the Cisco Unified CME router, a Cisco IOS CA on another router, or a third-party CA.</td>
</tr>
</tbody>
</table>
Phone Authentication

Phone Authentication Overview

registration authority (RA) Optional Cisco Unified CME phone authentication component, but it is required when a Cisco IOS CA is not on the Cisco Unified CME router itself or when the CA is a third-party CA. When present, the RA is able to offload some of the functions of the CA. Although an RA is often part of the CA server, the RA can also be an additional application, requiring an additional device to run it. The RA does not store any certificates; all certificates are stored by the CA. The RA has a trustpoint so that it can enroll with the CA.

The RA is the authority charged with recording or verifying some or all of the data required for the CA to issue certificates. In many cases the CA undertakes all of the RA functions itself, but where a CA operates over a wide geographical area or when there is security concern over exposing the CA at the edge of the network, it may be administratively advisable to delegate some of the tasks to an RA and leave the CA to concentrate on its primary tasks of signing certificates and certificate revocation lists.

certificate trust list (CTL) file A critical structure that contains the public key information (server identities) of all the servers with which the IP phone needs to interact (such as the Cisco Unified CME server, TFTP server, and CAPF server). The CTL file is digitally signed by the system administrator security token (SAST).

After you configure the CTL client, it creates the CTL file and makes it available in the TFTP directory. The CTL file is signed using the SAST certificate’s corresponding private key. An IP phone is then able to download this CTL file from the TFTP directory. The filename format for each phone’s CTL file is CTLSEP<mac-addr>.tlv.

When the CTL client is run on a router in the network that is not a Cisco Unified CME router, you must configure a CTL provider on each Cisco Unified CME router in the network. Similarly, if a CTL client is running on one of two Cisco Unified CME routers in a network, a CTL provider must be configured on the other Cisco Unified CME router. The CTL protocol transfers information to and from the CTL provider that allows the second Cisco Unified CME router to be trusted by phones and vice versa.

certificate revocation list (CRL) File that contains certificate expiration dates. It is used to determine whether a certificate that is presented is valid or revoked.

system administrator security token (SAST) Part of the CTL client that is responsible for signing the CTL file. The Cisco Unified CME certificate and its associated key pair are used for the SAST function. There are actually two SAST records pertaining to two different certificates in the CTL file for security reasons. They are known as SAST1 and SAST2. If one of the certificates is lost or compromised, then the CTL client regenerates the CTL file using the other certificate. When a phone downloads the new CTL file, it verifies with only one of the two original public keys that was installed earlier. This mechanism is to prevent IP phones from accepting CTL files from unknown sources.

<table>
<thead>
<tr>
<th>Component</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>registration authority (RA)</td>
<td>Optional Cisco Unified CME phone authentication component, but it is required when a Cisco IOS CA is not on the Cisco Unified CME router itself or when the CA is a third-party CA. When present, the RA is able to offload some of the functions of the CA. Although an RA is often part of the CA server, the RA can also be an additional application, requiring an additional device to run it. The RA does not store any certificates; all certificates are stored by the CA. The RA has a trustpoint so that it can enroll with the CA.</td>
</tr>
</tbody>
</table>
| certificate trust list (CTL) file | A critical structure that contains the public key information (server identities) of all the servers with which the IP phone needs to interact (such as the Cisco Unified CME server, TFTP server, and CAPF server). The CTL file is digitally signed by the system administrator security token (SAST).

After you configure the CTL client, it creates the CTL file and makes it available in the TFTP directory. The CTL file is signed using the SAST certificate’s corresponding private key. An IP phone is then able to download this CTL file from the TFTP directory. The filename format for each phone’s CTL file is CTLSEP<mac-addr>.tlv.

When the CTL client is run on a router in the network that is not a Cisco Unified CME router, you must configure a CTL provider on each Cisco Unified CME router in the network. Similarly, if a CTL client is running on one of two Cisco Unified CME routers in a network, a CTL provider must be configured on the other Cisco Unified CME router. The CTL protocol transfers information to and from the CTL provider that allows the second Cisco Unified CME router to be trusted by phones and vice versa. |
| certificate revocation list (CRL) | File that contains certificate expiration dates. It is used to determine whether a certificate that is presented is valid or revoked. |
| system administrator security token (SAST) | Part of the CTL client that is responsible for signing the CTL file. The Cisco Unified CME certificate and its associated key pair are used for the SAST function. There are actually two SAST records pertaining to two different certificates in the CTL file for security reasons. They are known as SAST1 and SAST2. If one of the certificates is lost or compromised, then the CTL client regenerates the CTL file using the other certificate. When a phone downloads the new CTL file, it verifies with only one of the two original public keys that was installed earlier. This mechanism is to prevent IP phones from accepting CTL files from unknown sources. |
Phone Authentication Overview

<table>
<thead>
<tr>
<th>Component</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>certificate authority proxy function (CAPF)</td>
<td>Entity that issues certificates (LSCs) to phones that request them. The CAPF is a proxy for the phones, which are unable to directly communicate with the CA. The CAPF can also perform the following certificate-management tasks:</td>
</tr>
<tr>
<td></td>
<td>• Upgrade existing locally significant certificates on the phones.</td>
</tr>
<tr>
<td></td>
<td>• Retrieve phone certificates for viewing and troubleshooting.</td>
</tr>
<tr>
<td></td>
<td>• Delete locally significant certificates on the phone.</td>
</tr>
<tr>
<td>manufacture-installed certificate (MIC)</td>
<td>Phones need certificates to engage in secure communications. Many phones come from the factory with MICs, but MICs may expire or become lost or compromised. Some phones do not come with MICs. LSCs are certificates that are issued locally to the phones using the CAPF server.</td>
</tr>
<tr>
<td>locally significant certificate (LSC)</td>
<td></td>
</tr>
<tr>
<td>transport layer security (TLS) protocol</td>
<td>IETF standard (RFC 2246) protocol, based on Netscape Secure Socket Layer (SSL) protocol. TLS sessions are established using a handshake protocol to provide privacy and data integrity.</td>
</tr>
<tr>
<td></td>
<td>The TLS record layer fragments and defragments, compresses and decompresses, and performs encryption and decryption of application data and other TLS information, including handshake messages.</td>
</tr>
</tbody>
</table>
To enable Cisco Unified CME phone authentication, the following steps occur:

1. Certificates are issued.
   
   The CA issues certificates to Cisco Unified CME, SAST, CAPF, and TFTP functions.

2. The CTL file is created, signed and published.
   
   a. The CTL file is created by the CTL client, which is configuration driven. Its goal is to create a CTLfile.tlv for each phone and deposit it in the TFTP directory. For the CTL client to complete its task, it needs the certificates and public key information of the CAPF server, Cisco Unified CME server, TFTP server, and SASTs.

   b. The CTL file is signed by the SAST credentials. There are two SAST records pertaining to two different certificates in the CTL file for security reasons. If one of the certificates is lost or compromised, then the CTL client regenerates the CTL file using the other certificate. When a phone downloads the new CTL file, it verifies the download with only one of the two original public keys that was installed earlier. This mechanism prevents IP phones from accepting CTL files from unknown sources.
c. The CTL file is published on the TFTP server. Because an external TFTP server is not supported in secure mode, the configuration files are generated by the Cisco Unified CME system itself and are digitally signed by the TFTP server’s credentials. The TFTP server credentials can be the same as the Cisco Unified CME credentials. If desired, a separate certificate can be generated for the TFTP function if the appropriate trustpoint is configured under the CTL-client interface.

3. The telephony service module signs phone configuration files and each phone requests its file.

4. When an IP phone boots up, it requests the CTL file (CTLfile.tlv) from the TFTP server and downloads its digitally signed configuration file, which has the filename format of SEP<mac-address>.cnf.xml.sgn.

5. The phone then reads the CAPF configuration status from the configuration file. If a certificate operation is needed, the phone initiates a TLS session with the CAPF server on TCP port 3804 and begins the CAPF protocol dialogue. The certificate operation can be an upgrade, delete, or fetch operation. If an upgrade operation is needed, the CAPF server makes a request on behalf of the phone for a certificate from the CA. The CAPF server uses the CAPF protocol to obtain the information it needs from the phone, such as the public key and phone ID. After the phone successfully receives a certificate from the server, the phone stores it in its flash memory.

6. With the certificate in its flash, the phone initiates a TLS connection with the secure Cisco Unified CME server on a well-known TCP port (2443), if the device security mode settings in the .cnf.xml file are set to authenticated or encrypted. This TLS session is mutually authenticated by both parties. The IP phone knows the Cisco Unified CME server’s certificate from the CTL file, which it initially downloaded from the TFTP server. The phone’s LSC is a trusted party for the Cisco Unified CME server, because the issuing CA certificate is present in the router.

**Operating in a Cisco Unified CME Phone Authentication Environment**

After setting up a Cisco Unified CME phone authentication environment, remember the following operational considerations:

- **Startup Messages**
- **Configuration File Maintenance**
- **CTL File Maintenance**

**Startup Messages**

If the certificate server is part of your startup configuration, you may see the following messages during the boot procedure:

% Failed to find Certificate Server’s trustpoint at startup
% Failed to find Certificate Server’s cert.

These messages are informational messages that indicate a temporary inability to configure the certificate server because the startup configuration has not been fully parsed yet. The messages are useful for debugging, in case the startup configuration has been corrupted.

You can verify the status of the certificate server after the boot procedure using the `show crypto pki server` command.
Configuration File Maintenance

In a secure environment, several types of configuration files must be digitally signed before they can be hosted and used. The filenames of all signed files have a .sgn suffix.

The Cisco Unified CME telephony service module creates phone configuration files (cnf.xml suffix) and hosts them on a Cisco IOS TFTP server. These files are signed by the TFTP server’s credentials.

In addition to the phone configuration files, other Cisco Unified CME configuration files such as the network and user-locale files must be signed. These files are internally generated by Cisco Unified CME, and the signed versions are automatically created in the current code path whenever the unsigned versions are updated or created.

Other configuration files that are not generated by Cisco Unified CME, such as ringlist.xml, distinctiveringlist.xml, audio files, and so forth, are often used for Cisco Unified CME features. Signed versions of these configuration files are not automatically created. Whenever a new configuration file that has not been generated by Cisco Unified CME is imported into Cisco Unified CME, use the `load-cfg-file` command, which does all of the following:

- Hosts the unsigned version of the file on the TFTP server.
- Creates a signed version of the file.
- Hosts the signed version of the file on the TFTP server.

You can also use the `load-cfg-file` command instead of the `tftp-server` command when only the unsigned version of a file needs to be hosted on the TFTP server.

CTL File Maintenance

The CTL file contains the SAST records, among other records. (A maximum of two SAST records may exist.) The CTL file is digitally signed by one of the SAST credentials that are listed in the CTL file before the CTL file is downloaded by the phone and saved in its flash. After receiving the CTL file, a phone trusts a newer or changed CTL file only if it is signed by one of the SAST credentials that is present in the original CTL file.

For this reason, you should take care to regenerate the CTL file only with one of the original SAST credentials. In the event that both SAST credentials are compromised and a CTL file must be generated with a new credential, you must reset the phone to its factory defaults.

Configuring Phone Authentication

To enable phone authentication for a Cisco Unified CME system, perform the following tasks.

**Note**

Tasks 1 through 3 are standard PKI configuration tasks. Suggested configurations are included here for ease of use, but you should refer to the PKI documentation for complete information. See the “Implementing and Managing a PKI” section of the *Cisco IOS Security Configuration Guide*. 
<table>
<thead>
<tr>
<th>Task</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. <strong>Provisioning a Cisco IOS Certification Authority, page 158</strong></td>
<td>Standard PKI commands are used to configure a Cisco IOS router as a CA server. The CA server can be located on the Cisco Unified CME router or on an external router. If you use a third-party CA, follow the provider’s instructions instead of performing this task.</td>
</tr>
<tr>
<td>2. <strong>Configuring a Registration Authority, page 162</strong></td>
<td>(Optional) If the CA server is not located on the Cisco Unified CME router, you need to configure an RA server on the Cisco Unified CME router. Standard PKI commands are used to configure an RA on the Cisco Unified CME router.</td>
</tr>
</tbody>
</table>
| 3. **Provisioning Certificates for Cisco Unified CME Server Functions, page 165** | The Cisco Unified CME server needs certificates to carry out the following tasks:  
  * Establish TLS sessions with the phones for secure SCCP signaling on TCP port 2443  
  * Establish TLS sessions between the phones and the CAPF for phone certificate operations  
  * Digitally sign phone configuration files  
  * Have the CTL files signed by the CTL client (SAST function)  
Standard PKI commands are used to configure these certificates. |
| 4. **Manually Importing MIC Root Certificate on the Cisco Unified CME Router, page 168** | (Optional) The MIC root certificate must be present in the Cisco Unified CME router to allow Cisco Unified CME to authenticate the MIC that is presented to it. This task should be performed only if one of the following situations exists:  
  * If you choose to use MIC as the method for phone authentication during CAPF certificate operation  
  * If you plan to establish the TLS session for SCCP signaling using the phone’s MIC instead of an LSC |
| 5. **Configuring Telephony-Service Security Parameters, page 173** | Secure communications are enabled per phone or globally and trustpoints with valid certificates are specified. |
| 6. **Configuring the CTL Client and CTL Provider, page 179** | The credentials of various functions are included in the CTL file, which is then created and hosted on the TFTP server. |
| 7. **Configuring the CAPF Server, page 187** | The CAPF server is set up on the Cisco Unified CME router and the type of authentication to use when upgrading phone certificates is specified. |
| 8. **Entering the Authentication String on the Phone, page 191** | (Optional) When the authentication-string method has been chosen for the authentication when updating LSCs, a phone user must manually enter the authentication string on the phone. |
Prerequisites

Set the system clock using one of these methods:

- Configure Network Time Protocol (NTP).
- Manually set the software clock using the `clock set` command.

Both methods are explained in the “Performing Basic System Management” chapter of the *Cisco IOS Network Management Configuration Guide*.

Provisioning a Cisco IOS Certification Authority

This task configures a root certificate server, also called a certification authority or CA, on a Cisco IOS router. The router can be the Cisco Unified CME router or an external router. If an external router is used, a registration authority (RA) must be configured on the Cisco Unified CME router, as described in the “Configuring a Registration Authority” section on page 162.

A trustpoint for the CA is automatically generated by the router when the CA is started. You can create your own trustpoint, using the same label as the label in the `crypto pki server` command, if you need to use a specific RSA key for the CA. If the router sees a configured trustpoint with the same label as that of the “crypto pki server,” it uses this trustpoint and does not automatically create a trustpoint.

Setting up a Cisco IOS CA is a standard PKI task. The basic steps are included here for ease of use. For more information, see the “Configuring and Managing a Cisco IOS Certificate Server for PKI Deployment” section in “Part 5: Implementing and Managing a PKI” in the *Cisco IOS Security Configuration Guide*.

Perform the following steps on the Cisco IOS router on which the CA is being installed.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `ip http server`
4. `crypto pki server label`
5. `database level {minimal | names | complete}`
6. `database url root-url`
7. `lifetime certificate time`
8. `issuer-name CN=label`
9. `exit`

---

*Note* If you use a third-party CA, follow the provider’s instructions instead of performing this task.

*Note* The `grant auto` command allows certificates to be issued automatically. You can use it when testing and building simple networks, and it should be used only for that purpose. A security best practice is to disable this functionality using the `no grant auto` command when configuration is complete, so that certificates are not automatically granted.
10. crypto pki trustpoint *label*
11. enrollment url *ca-url*
12. exit
13. crypto pki server *label*
14. grant auto
15. no shutdown
16. exit

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
- Enter your password if prompted. |
| **Example:** Router> enable |
| **Step 2** configure terminal | Enters global configuration mode. |
| **Example:** Router# configure terminal |
| **Step 3** ip http server | Enables the Cisco web-browser user interface on the local Cisco Unified CME router. |
| **Example:** Router(config)# ip http server |
| **Step 4** crypto pki server *label* | Defines a label for the certificate server and enters certificate-server configuration mode.  
- *label*—Name for CA certificate server. |
| **Example:** Router(config)# crypto pki server cisco1 |
| **Step 5** database level (minimal | (Optional) Controls what type of data is stored in the certificate enrollment database. The default if this command is not used is *minimal*.  
- *minimal*—Enough information is stored only to continue issuing new certificates without conflict; the default value.  
- *names*—In addition to the information given in the minimal level, the serial number and subject name of each certificate.  
- *complete*—In addition to the information given in the minimal and names levels, each issued certificate is written to the database.  

**Note** The *complete* keyword produces a large amount of information; if it is issued, you should also specify an external TFTP server in which to store the data by means of the *database url* command. |
| names | complete) |  |  | |
### Command or Action

#### Step 6
database url root-url

**Example:**
```bash
Router(config-cs-server)# database url nvram:
```

(Optional) Specifies the location where all database entries for the certificate server are to be written out. If this command is not specified, all database entries are written to NVRAM.

**Note**
- *root-url*—Location where database entries will be written out. The URL can be any URL that is supported by the Cisco IOS file system (IFS).

**Note**
- If the CA is going to issue a large number of certificates, select an appropriate storage location like flash or other storage device to store the certificates.

**Note**
- When the storage location chosen is flash and the file system type on this device is Class B (LEFS), make sure to check free space on the device periodically and use the `squeeze` command to free the space used up by deleted files. This process may take several minutes and should be done during scheduled maintenance periods or off-peak hours.

#### Step 7
lifetime certificate time

**Example:**
```bash
Router(config-cs-server) lifetime certificate 888
```

(Optional) Specifies the lifetime, in days, of certificates issued by this CA server.

**Note**
- *time*—Number of days until a certificate expires. Range is from 1 to 1825. Default is 1 year. The maximum certificate lifetime is 1 month less than the lifetime of the CA certificate.

**Note**
- If this command is used, it must be used before the server is enabled with the `no shutdown` command.

#### Step 8
issuer-name CN=name

**Example:**
```bash
Router(config-cs-server)# issuer-name CN=cisco1
```

(Optional) Specifies a distinguished name (DN) as the certification-authority (CA) issuer name for the certificate server.

If the issuer name is not configured, CN = CA label.

#### Step 9
exit

**Example:**
```bash
Router(config-cs-server)# exit
```

Exits certificate-server configuration mode.

#### Step 10
crypto pki trustpoint label

**Example:**
```bash
Router(config)# crypto pki trustpoint cisco1
```

(Optional) Declares a trustpoint and enters ca-trustpoint configuration mode.

**Note**
- *label*—Name for the trustpoint.

**Note**
- Use this command and the `enrollment url` command if this CA is local to the Cisco Unified CME router. These commands are not needed for a CA running on an external router.
Configuring Phone Authentication

1. Use the `show crypto pki server` command to display the status of the certificate server.

   Example:
   ```
   Router(config-ca-trustpoint)# show crypto pki server
   ```

2. Use the `show running-config` command to display the running configuration, including the certificate-server configuration.

   Example:
   ```
   Router(config)# show running-config
   ```

### Examples

The following example defines a CA named cisco1 running locally on the Cisco Unified CME router:

```plaintext
ip http server

crypto pki server cisco1
database level complete
database url nvram:
```
crypto pki trustpoint cisco1
  enrollment url http://ca-server.company.com

crypto pki server cisco1
  no grant auto
  no shutdown

Configuring a Registration Authority

Note
This task is required if the CA is a third-party CA or if the CA is a Cisco IOS CA on a router external to the Cisco Unified CME router. In these cases, the CAPF server requires an RA to issue certificates to the phone.

The RA is the authority charged with recording or verifying some or all of the data required for the CA to issue certificates. In many cases the CA undertakes all of the RA functions itself, but where a CA operates over a wide geographical area or when there is security concern over exposing the CA at the edge of the network, it may be administratively advisable to delegate some of the tasks to an RA and leave the CA to concentrate on its primary tasks of signing certificates.

You can configure a Cisco IOS certificate server to run in RA mode. When the RA receives a manual or Simple Certificate Enrollment Protocol (SCEP) enrollment request, the administrator can either reject or grant it on the basis of local policy. If the request is granted, it is forwarded to the issuing CA, and the CA automatically generates the certificate and returns it to the RA. The client can later retrieve the granted certificate from the RA.

Note that setting up an RA and trustpoint are standard PKI tasks. The steps are included here for ease of use. For more information, see the “Implementing and Managing a PKI” section in the Cisco IOS Security Configuration Guide.

Perform these steps on the Cisco Unified CME router.

Note
The grant auto command allows certificates to be issued automatically. You should only use it when testing and building simple networks. A security best practice is to disable this functionality using the no grant auto command when configuration is complete, so that certificates cannot be continually granted.

SUMMARY STEPS

1. enable
2. configure terminal
3. crypto pki trustpoint label
4. enrollment url ca-url
5. revocation-check method1 [method2][method3]
6. serial-number [none]
7. rsakeypair key-label [key-size [encryption-key-size]]
8. exit
9. crypto pki server label
10. mode ra
11. lifetime certificate time
12. grant auto
13. no shutdown
14. exit

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td>Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> crypto pki trustpoint label</td>
<td>Declares the trustpoint that your RA mode certificate server should use and enters CA-trustpoint configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# crypto pki trustpoint ra12</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> enrollment url ca-url</td>
<td>Specifies the enrollment URL of the issuing CA certificate server (root certificate server).</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-ca-trustpoint)# enrollment url</td>
<td></td>
</tr>
<tr>
<td><a href="http://ca-server.company.com">http://ca-server.company.com</a></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> revocation-check method1 [method2[method3]]</td>
<td>(Optional) Checks the revocation status of a certificate and specifies one or more methods to check the status. If a second and third method are specified, each method is used only if the previous method returns an error, such as a server being down. Valid values for methodn are as follows:</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-ca-trustpoint)# revocation-check</td>
<td></td>
</tr>
<tr>
<td>none</td>
<td></td>
</tr>
</tbody>
</table>
Configuring Phone Authentication

### Command or Action

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| 6    | `serial-number [none]` | (Optional) Specifies whether the router serial number should be included in the certificate request. If this command is not used, you are prompted for the serial number during certificate enrollment.  
  - `none`—(Optional) A serial number is not included in the certificate request. |
| 7    | `rsakeypair key-label [key-size [encryption-key-size]]` | (Optional) Specifies an RSA key pair to use with a certificate.  
  - `key-label`—Name of the key pair, which is generated during enrollment if it does not already exist or if the `auto-enroll regenerate` command is used.  
  - `key-size`—(Optional) Size of the desired RSA key. If not specified, the existing key size is used.  
  - `encryption-key-size`—(Optional) Size of the second key, which is used to request separate encryption, signature keys, and certificates. |
| 8    | `exit` | Exits ca-trustpoint configuration mode. |
| 9    | `crypto pki server label` | Defines a label for the certificate server and enters certificate-server configuration mode.  
  - `label`—Name for the trustpoint and RA. The certificate-server label must have the same name as the trustpoint that was created in Step 3. |
| 10   | `mode ra` | Places the PKI server into certificate-server mode for the RA. |
| 11   | `lifetime certificate time` | (Optional) Specifies the lifetime, in days, of a certificate.  
  - `time`—Number of days until the certificate expires. Range is from 1 to 1825. Default is 1 year. The maximum certificate lifetime is 1 month less than the lifetime of the CA certificate.  
  - Note: If this command is used, it must be used before the server is enabled with the `no shutdown` command. |
| 12   | `grant auto` | Allows an automatic certificate to be issued to any requestor.  
  - Note: Use this command only during enrollment when testing and building simple networks. A security best practice is to disable this functionality after configuration using the `no grant auto` command so that certificates cannot be continually granted. |
Verifying the Registration Authority

**Step 1**  
Use the `show crypto pki server` command to display the status of the certificate server.

**Step 2**  
Use the `show crypto pki certificates` command to display certificate information.

**Step 3**  
Use the `show running-config` command to display the running configuration.

### Examples

The following example sets up an RA and trustpoint named ra12:

```bash
Router(config)# crypto pki trustpoint ra12
Router(config-ca-trustpoint)# enrollment url http://ca-server.company.com
Router(config-ca-trustpoint)# revocation-check none
Router(config-ca-trustpoint)# rsakeypair exampleCAkeys 1024 1024
Router(config-ca-trustpoint)# exit
Router(config)# crypto pki server ra12
Router(config-cs-server)# mode ra
Router(config-cs-server)# lifetime certificate 1800
Router(config-cs-server)# no grant auto
Router(config-cs-server)# no shutdown
Router(config-cs-server)# exit
```

The following example sets up a trustpoint named sast2 that periodically generates a CRL instead of having it generated manually. Third-party CAs may require this functionality.

```bash
Router(config)# crypto pki trustpoint sast2
Router(config-ca-trustpoint)# enrollment url http://NTP-ab11:80
Router(config-ca-trustpoint)# serial-number
Router(config-ca-trustpoint)# revocation-check crl
Router(config-ca-trustpoint)# rsakeypair sast2
```

### Provisioning Certificates for Cisco Unified CME Server Functions

The Cisco Unified CME router needs certificates for the following server functions:

- **Secure SCCP server (Cisco Unified CME)**—Requires a certificate for TLS sessions with phones.
- **TFTP server credentials**—Requires a key pair and certificate for signing configuration files.
• CAPF server—Requires a certificate for TLS sessions with phones.
• Security tokens—Required for signing the CTL file. Cisco recommends creating two certificates, one for primary use and the other for backup.

For each of the above functions, perform the steps in this section to obtain a certificate.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. crypto pki trustpoint trustpoint-label
4. enrollment url url
5. revocation-check method1 [method2][method3]
6. rsakeypair key-label [key-size [encryption-key-size]]
7. exit
8. crypto pki authenticate trustpoint-label
9. crypto pki enroll trustpoint-label
10. Repeat Step 3 through Step 9 for each server function that requires a certificate.

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td>Enter your password if prompted.</td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3 crypto pki trustpoint trustpoint-label</td>
<td>Declares the trustpoint that the Cisco Unified CME certificate server should use and enters ca-trustpoint configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# crypto pki trustpoint capf</td>
<td></td>
</tr>
<tr>
<td>Step 4 enrollment url url</td>
<td>Specifies the enrollment URL of the issuing CA certificate server (root certificate server).</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-ca-trustpoint)# enrollment url</td>
<td><a href="http://ca-server.company.com">http://ca-server.company.com</a></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Step 5 \texttt{revocation-check method1 [method2[method3]]}</td>
<td>(Optional) Checks the revocation status of a certificate.</td>
</tr>
<tr>
<td>\textbf{Example:} Router(config-ca-trustpoint)# revocation-check none</td>
<td>- \texttt{method}—Method used by the router to check the revocation status of the certificate. If a second and third method are specified, each method is used only if the previous method returns an error, such as a server being down.</td>
</tr>
<tr>
<td>Step 6 \texttt{rsakeypair key-label [key-size [encryption-key-size]]}</td>
<td>(Optional) Specifies a key pair to use with a certificate.</td>
</tr>
<tr>
<td>\textbf{Example:} Router(config-ca-trustpoint)# rsakeypair capf 1024 1024</td>
<td>- \texttt{key-label}—Name of the key pair, which is generated during enrollment if it does not already exist or if the \texttt{auto-enroll regenerate} command is configured.</td>
</tr>
<tr>
<td>Step 7 \texttt{exit}</td>
<td>Exits CA trustpoint configuration mode.</td>
</tr>
<tr>
<td>\textbf{Example:} Router(config-ca-trustpoint)# exit</td>
<td>- \texttt{key-size}—(Optional) Size of the desired RSA key. If not specified, the existing key size is used.</td>
</tr>
<tr>
<td>Step 8 \texttt{crypto pki authenticate trustpoint-label}</td>
<td>Retrieves the CA certificate and authenticates it. Checks the certificate fingerprint if prompted.</td>
</tr>
<tr>
<td>\textbf{Example:} Router(config)# crypto pki authenticate capf</td>
<td>- \texttt{trustpoint-label}—Trustpoint label.</td>
</tr>
<tr>
<td>Step 9 \texttt{crypto pki enroll trustpoint-label}</td>
<td>Enrolls with the CA and obtains the certificate for this trustpoint.</td>
</tr>
<tr>
<td>\textbf{Example:} Router(config)# crypto pki enroll capf</td>
<td>- \texttt{trustpoint-label}—Trustpoint label.</td>
</tr>
<tr>
<td>Step 10 Repeat Step 3 through Step 9 for each server function that requires a certificate.</td>
<td>—</td>
</tr>
</tbody>
</table>
Verifying Certificates for Server Functions

**Step 1**
Use the `show crypto pki certificates` command to display information about the certificates.

**Step 2**
Use the `show running-config` command to display the running configuration.

**Examples**

The following example establishes a trustpoint for the CAPF server called capf.

```
Router(config)# crypto pki trustpoint capf
Router(config-ca-trustpoint)# enrollment url http://ca-server.company.com
Router(config-ca-trustpoint)# revocation-check none
Router(config-ca-trustpoint)# rsakeypair capf 1024 1024
Router(config-ca-trustpoint)# exit
Router(config)# crypto pki authenticate capf
Router(config)# crypto pki enroll capf
```

**Manually Importing MIC Root Certificate on the Cisco Unified CME Router**

When a phone uses a MIC for authentication during the TLS handshake with the CAPF server, the CAPF server must have a copy of the MIC in order to verify it. Different certificates are used for different types of IP phones.

A phone uses a MIC for authentication when it has a MIC but no LSC. For example, you have a Cisco Unified IP Phone 7970 that has a MIC by default but no LSC. When you schedule a certificate upgrade with the authentication mode set to MIC for this phone, the phone presents its MIC to the Cisco Unified CME CAPF server for authentication. The CAPF server must have a copy of the MIC's root certificate to verify the phone's MIC. Without this copy, the CAPF upgrade operation fails.

To ensure that the CAPF server has copies of the MICs it needs, you must manually import certificates to the CAPF server as described in this section. The number of certificates that you need to import depends on your network configuration. Manual enrollment refers to copy-and-paste or TFTP transfer methods.

Repeat the enrollment procedure for each type of phone that requires a MIC for authentication.

For more information, see the “Configuring Cut-and-Paste Certificate Enrollment” section of the “Configuring Certificate Enrollment for a PKI” chapter in the *Cisco IOS Security Configuration Guide*.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `crypto pki trustpoint name`
4. `revocation-check method1`
5. `enrollment terminal`
6. `exit`
7. `crypto pki authenticate name`
8. Open the MIC root file and copy the certificate.
9. When prompted, paste the certificate, press Enter, and type `quit`.
10. Enter `y` to accept the certificate.
11. Repeat Step 3 through Step 10 for each additional phone type.

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
• Enter your password if prompted. |
| **Example:** Router> enable | |
| **Step 2** configure terminal | Enters global configuration mode. |
| **Example:** Router# configure terminal | |
| **Step 3** crypto pki trustpoint name | Declares the CA that your router should use and enters CA-trustpoint configuration mode.  
• `name`—CA trustpoint name. |
| **Example:** Router(config)# crypto pki trustpoint cisco1 | |
| **Step 4** revocation-check method1 | Checks the revocation status of a certificate.  
• `method1`—The method used by the router to check the revocation status of the certificate. For this task, the only available method is `none`. The keyword `none` means that a revocation check is not performed and the certificate is always accepted.  
**Note** Using the `none` keyword is mandatory for this task. |
| **Example:** Router(ca-trustpoint)# revocation-check none | |
| **Step 5** enrollment terminal | Specifies manual (copy-and-paste) certificate enrollment. |
| **Example:** Router(ca-trustpoint)# enrollment terminal | |
| **Step 6** exit | Exits CA-trustpoint configuration mode. |
| **Example:** Router(ca-trustpoint)# exit | |
| **Step 7** crypto pki authenticate name | Authenticates the CA (by getting the certificate from the CA).  
• `name`—Name of the CA. |
| **Example:** Router(config)# | |
| **Step 8** Open the MIC root file and copy the certificate. | The MIC root file is a file with name a*.0, located in the directory `C:\Program Files\Cisco\Certificates`  
Copy to a buffer or temporary location all of the contents that appear between “-----BEGIN CERTIFICATE-----” and “-----END CERTIFICATE-----”. |
Configuring Phone Authentication

Examples

The following example shows three certificates imported to the router (7970, 7960, PEM).

```
Router(config)# crypto pki trustpoint 7970
Router(ca-trustpoint)# revocation-check none
Router(ca-trustpoint)# enrollment terminal
Router(ca-trustpoint)# exit
Router(config)# crypto pki authenticate 7970
```

Certificate has the following attributes:

Fingerprint MD5: F7E150EA 5E6E3AC5 615FC696 66415C9F
Fingerprint SHA1: 1BE2B503 DC72EE28 0C0F6B18 798236D8 D3B18BE6

% Do you accept this certificate? [yes/no]: y
Trustpoint CA certificate accepted.
% Certificate successfully imported

```
Router(config)# crypto pki trustpoint 7960
Router(ca-trustpoint)# revocation-check none
Router(ca-trustpoint)# enrollment terminal
Router(ca-trustpoint)# exit
Router(config)# crypto pki authenticate 7960
```

Certificate has the following attributes:

Fingerprint MD5: F7E150EA 5E6E3AC5 615FC696 66415C9F
Fingerprint SHA1: 1BE2B503 DC72EE28 0C0F6B18 798236D8 D3B18BE6

% Do you accept this certificate? [yes/no]: y
Trustpoint CA certificate accepted.
% Certificate successfully imported

```
Repeat Step 3 through Step 10 for each additional phone type.
```
GjAYBgNVBAYTAlNUcnVzdGRvcl1vcmwGCSqGSIb3DQEBCwUAA4GBA6r5O76/a2W7MmX9Q7tQcGis15Lx0t1H3s4nYQldKdSb9jKm48C9JeKdU5y7J6OeI1DkG2Q9Y8QH86f95+JcC6vWtHfIVg8QHuhsRzCPjTtTqHz8cKoVWJOI5h77o5RZr6ZKsKjiJ4zRv3p1wZG8UtO3vD9/hngI
quit
Certificate has the following attributes:
Fingerprint MD5: 4B9636DF 0F3BA6B7 5F54BE72 24762DBC
Fingerprint SHA1: A917775F 868B37A5 C130ED28 268E3C2D
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported

Router(config)# crypto pki trustpoint PEM
Router(config-trustpoint)# revocation-check none
Router(config-trustpoint)# enrollment terminal
Router(config-trustpoint)# exit
Router(config)# crypto pki authenticate PEM
Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
MIIDqDCAAFAIBAgIQcDhL5VBU9b5QoAkb4cZPcjakJQCAZgkQhkiG9w0BAQFAQFADaUMRywFAYDBQQKW1dxXZ3yBfX9N2Nz1XzMQwBqYVdQDQDEWtDQXATU1RLtA1WTXe
Pw0wMz1qMDYzIe1NTMwv80zA2MDYzIe1NTMwv80z2MDYzIe1NTMwv80z3MDYzIe1NTMwv80z4MDYzIe1NTMwv80z5MDYzIe1NTMwv80z6MDYzIe1NTMwv80z7MDYzIe1NTMwv80z8MDYzIe1NTMwv80z9MDYzIe1NTMwv80zA0MDYzIe1NTMwv80zA1MDYzIe1NTMwv80zA2MDYzIe1NTMwv80zA3MDYzIe1NTMwv80zA4MDYzIe1NTMwv80zA5MDYzIe1NTMwv80zA6MDYzIe1NTMwv80zA7MDYzIe1NTMwv80zA8MDYzIe1NTMwv80zA9MDYzIe1NTMwv80zAA0MDYzIe1NTMwv80zAA1MDYzIe1NTMwv80zAA2MDYzIe1NTMwv80zAA3MDYzIe1NTMwv80zAA4MDYzIe1NTMwv80zAA5MDYzIe1NTMwv80zAA6MDYzIe1NTMwv80zAA7MDYzIe1NTMwv80zAA8MDYzIe1NTMwv80zAA9MDYzIe1NTMwv80zAACMDYzIe1NTMwv80zAADMDYzIe1NTMwv80zAAEMDVQQKEw1DaXNjbyBTeXN0ZW1zMRQwEgYDVQQDEwtDQVAtUlRQLTAwMTAeFw0wMzAyMDYyMzI3MTNaFw0yMzAyMDYyMzM2MzRaMC4xFjAUBgNVBAsTGGl0ZSBDb3VwcGxvYXRpb24gU2lib3NlIENvZmVjdCBzaXNjaWVzcyB0ZXN0IHRlZmF1bHQgQXV0aG9yaW5ncyB0aGlzIHRoZSB2YWxvc2UgU2lyb2NyaXZlIHN0cmluZwYDVQJBMQGCCsGAQUFBwIxc3BhY2VzcyA9BgNVBAoTDUNpc2NvIEN5c3RlbXMgSW5jMRUwEwYDVQQDEwxDQVBGLTdvcmxQ0FwZzEYMBYGA1UEAwwGDGcCIG9wIEZvcmQKIENvZmVjdCBfMDgTBGkVaHJlZ3MgU2FtcGxlIENvZmVjdCBfMDEwJwYDVQQDDAsbQiBDb3VwcGxvYXRpb24gUHJvZ3JhbWQgUElOIEtBIENvZmVjdCBjMTAdBgNVBAcTBUNpc2NvIFN5c3RlbXMgSW5jMRUwEwYDVQQDEwFJ1N0ZS5WczAwHhcNMDQwNzE1MjIzODMyWhcNMTkwNzEyMjIzODMxWjBAMQswCQYDVQQGEwJVUzEaMBgGA1UdJQQMBQGCCsGAQUFBwIBBjAGA1UEChMDS2hpbmFuZCBbb25nIEFwc2lkcyBDYWdpbmcgU29tbWVudFBsZmlyZXMgUHJvZ3JhbCBQcm9tZWRpYSBQbGVhc2UgQ29udGFpbmcgRGlnaXZlLiBDQTAeMBgGA1UdDgICVzAxFDBkMTQwNzA0MjAxMDk0MA0GCSqGSIb3DQEBCwUAA4GCSqGSIb3DQEBCwUDBxQzI2MB8GA1UdDgEB/wQIKQDhC+gYDVR0PAQH/BAQDAgWkJfJraS0vJr9S7o2BPRTG28Z6wDQ==
quilt
Certificate has the following attributes:
Fingerprint MD5: 233C8E33 8632EA4E 76D79FEB FFB7962C
Fingerprint SHA1: F7B40B94 5831D2AB 474AB8F2 25990732 227631BE
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported
Use the `show crypto pki trustpoint status` command to show that enrollment has succeeded and that five CA certificates were granted. The five certificates include the three certificates just entered and the CA server certificate and the router certificate.

Router# `show crypto pki trustpoint status`

Trustpoint 7970:
Issuing CA certificate configured:
Subject Name:
cn=CAP-RTP-002,o=Cisco Systems
Fingerprint MD5: F7E150EA 5E6E3AC5 615FC696 66415C9F
Fingerprint SHA1: 1BE2B503 DC72EE28 0C0F6B18 798236D8 D3B18BE6
State:
Keys generated ............ Yes (General Purpose)
Issuing CA authenticated .... Yes
Certificate request(s) ...... None
Trustpoint 7960:
Issuing CA certificate configured:
Subject Name:
cn=CAPF-508A3754,o=Cisco Systems Inc,c=US
Fingerprint MD5: 6BAE18C2 0BCE391E DAE2FE4C 5810F576
Fingerprint SHA1: B7735A2E 3A5C274F C311D7F1 3BE89942 355102DE
State:
Keys generated ............ Yes (General Purpose)
Issuing CA authenticated .... Yes
Certificate request(s) ...... None
Trustpoint PEM:
Issuing CA certificate configured:
Subject Name:
cn=CAP-RTP-001,o=Cisco Systems
Fingerprint MD5: 233C8E33 8632EA4E 76D79FEB FF0B51C6
Fingerprint SHA1: F7B40B94 5831D2AB 447AB8F2 25990732 227631BE
State:
Keys generated ............ Yes (General Purpose)
Issuing CA authenticated .... Yes
Certificate request(s) ...... None
Trustpoint srstcaserver:
Issuing CA certificate configured:
Subject Name:
cn=srstcaserver
Fingerprint MD5: 6AF5B084 79C93F2B 76CC8FE6 8781AF5E
Fingerprint SHA1: 47D30503 38FF1524 711448B4 9763FAF6 3A8E7DCF
State:
Keys generated ............ Yes (General Purpose)
Issuing CA authenticated .... Yes
Certificate request(s) ...... None

Trustpoint srstca:
Issuing CA certificate configured:
Subject Name:
cn=srstcaserver
Fingerprint MD5: 6AF5B084 79C93F2B 76CC8FE6 8781AF5E
Fingerprint SHA1: 47D30503 38FF1524 711448B4 9763FAF6 3A8E7DCF
Router General Purpose certificate configured:
Subject Name:
serialNumber=F3246544+hostname=c2611XM-sSRST.cisco.com
Fingerprint: 35471295 1C907EC1 45B347BC 7A9C4BB6
State:
Keys generated ........... Yes (General Purpose)
Issuing CA authenticated .... Yes
Certificate request(s) ...... Yes
Configuring Telephony-Service Security Parameters

The commands in this task define security parameters for phones and allow you to enable security per phone or globally.

**Note**
If you select the authentication string method of authentication in the `cert-oper` command, you must also enter an authentication string at each phone that is receiving an updated LSC. For instructions on this task, see the “Entering the Authentication String on the Phone” section on page 191.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `telephony-service`
4. `secure-signaling trustpoint label`
5. `tftp-server-credentials trustpoint label`
6. `device-security-mode {authenticated | none}`
7. `cnf-file perphone`
8. `load-cfg-file file-url alias file-alias [sign] [create]`
9. `server-security-mode {secure | non-secure}`
10. `exit`
11. `ephone phone-tag`
12. `device-security-mode {authenticated | none}`
13. `capf-auth-str digit-string`
14. `cert-oper {delete | fetch | upgrade} auth-mode {auth-string | LSC | MIC | null-string}`
15. `reset`
16. `exit`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router&gt; enable</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router# configure terminal</code></td>
<td></td>
</tr>
</tbody>
</table>
### Configuring Phone Authentication

#### Step 3
**telephony-service**

**Example:**
```config
Router(config)# telephony-service
```

Enters telephony-service configuration mode.

#### Step 4
**secure-signaling trustpoint label**

**Example:**
```config
Router(config-telephony)# secure-signaling trustpoint cme-sccp
```

Specifies the name of the PKI trustpoint that has the valid certificate to be used for TLS handshakes with IP phones on TCP port 2443.

- **label**—Name of a configured PKI trustpoint with a valid certificate.

#### Step 5
**tftp-server-credentials trustpoint label**

**Example:**
```config
Router(config-telephony)# tftp-server-credentials trustpoint cme-tftp
```

Specifies the name of the PKI trustpoint to be used to sign the phone configuration files. This can be the CAPF-server trustpoint that was used in the previous step or any trustpoint with a valid certificate.

- **label**—Name of a configured PKI trustpoint with a valid certificate.

#### Step 6
**device-security-mode (authenticated | none)**

**Example:**
```config
Router(config-telephony)# device-security-mode authenticated
```

Enables security mode for all security-capable phones in the system.

- **authenticated**—SCCP signaling between a device and Cisco Unified CME takes place through the secure TLS connection on TCP port 2443.
- **none**—SCCP signaling is not secure. This is the default.

**Note** The setting you make in this command can be overridden for individual ephones by using the `device-security-mode` command in ephone configuration mode.

#### Step 7
**cnf-file perphone**

**Example:**
```config
Router(config-telephony)# cnf-file perphone
```

Specifies the generation of a separate configuration file for each individual phone. Separate configuration files for each endpoint are required for security.
### Configuring Phone Authentication

#### Step 8

**load-cfg-file** file-url alias file-alias [sign] [create]

Example:
```
Router(config-telephony)# load-cfg-file
slot0:Ringlist.xml alias Ringlist.xml sign create
```

(Optional) Signs configuration files that are not created by Cisco Unified CME. Also loads the signed and unsigned versions of a file on the TFTP server. To simply serve an already signed file on the TFTP server, use this command without the `sign` and `create` keywords.

- **file-url** — Complete path of a configuration file in a local directory.
- **alias file-alias** — Alias name of the file to be served on the TFTP server.
- **sign** — (Optional) The file needs to be digitally signed and served on the TFTP server.
- **create** — (Optional) Creates the signed file in the local directory.

**Note**

The first time that you use this command for each file, use the `create` keyword in addition to the `sign` keyword. The `create` keyword is not maintained in the running configuration to prevent signed files from being recreated during every reload.

#### Step 9

**server-security-mode** (secure | non-secure)

Example:
```
Router(telephony)# server-security-mode secure
```

(Optional) Changes the security mode of the server.

- **secure** — Secure mode.
- **non-secure** — Non-secure mode.

**Note**

This command has no effect until the CTL file is initially generated by the CTL client. When the CTL file is generated, the CTL client automatically sets the server security mode to secure. You can toggle the mode thereafter.

**Note**

This command must be followed by the `regenerate` command in CTL-client configuration mode.

#### Step 10

**exit**

Example:
```
Router(config)# exit
```

Exits telephony-service configuration mode.

#### Step 11

**ephone** phone-tag

Example:
```
Router(config)# ephone 24
```

Enters ephone configuration mode.

- **phone-tag** — Identifier of the ephone to be configured.
### Configuring Phone Authentication

**Step 12**

**device-security-mode** *(authenticated | none)*

**Example:**

Router(config-ephone)# device-security-mode authenticated

(Optional) Sets the security mode for SCCP signaling for an ephone communicating with the Cisco Unified CME router.

- **authenticated**—SCCP signaling between a device and Cisco Unified CME takes place through the secure TLS connection on TCP port 2443.
- **none**—SCCP signaling is not secure.

**Note** You can set this value globally using the `device-security-mode` command in telephony-service configuration mode. A per-phone setting in ephone configuration mode overrides the global setting for that phone.

**Step 13**

**capf-auth-str** *(digit-string)*

**Example:**

Router(config-ephone)# capf-auth-str 2734

(Optional) Defines a string to use as a personal identification number (PIN) for CAPF authentication. Use the show `capf-server auth-string` command to display configured strings. For instructions on how to enter the string from the phone, see the “Entering the Authentication String on the Phone” section on page 191.

- **digit-string**—String of digits that the phone user must dial for CAPF authentication. The string can be from 4 to 10 digits in length.

**Note** You can set this value globally using this command or per ephone using the `auth-string` command in CAPF-server configuration mode.
## Step 14: Configuring Phone Authentication

**Command or Action**

| cert-oper {delete | fetch | upgrade} auth-mode {auth-string | LSC | MIC | null-string} |

**Example:**

Router(config-ephone)# cert-oper upgrade auth-mode auth-string

**Purpose**

(Optional) Initiates the indicated certificate operation on this ephone.

- **delete**—Removes the phone certificate.
- **fetch**—Retrieves the phone certificate for troubleshooting.
- **upgrade**—Upgrades the phone certificate.
- **auth-mode**—Type of authentication to use during CAPF sessions to verify endpoints that request certificates.
- **auth-string**—The phone user enters a special authentication string at the phone. The string is set with the `capf-auth-str` command and is provided to the phone user by the system administrator.
- **LSC**—The phone provides its phone certificate for authentication. Precedence is given to an LSC if one exists.
- **MIC**—The phone provides its phone certificate for authentication. Precedence is given to an MIC if one exists. If this option is chosen, the MIC’s issuer certificate must be imported into a PKI trustpoint. See the “Manually Importing MIC Root Certificate on the Cisco Unified CME Router” section on page 168.
- **null-string**—No authentication.

**Note**

You can initiate certificate operations globally using the `cert-oper` command in CAPF-server configuration mode. You can set authentication mode globally using the `auth-mode` command in CAPF-server configuration mode.

## Step 15: reset

**Example:**

Router(config-ephone)# reset

**Purpose**

Performs a complete reboot of the phone.

## Step 16: exit

**Example:**

Router(config-ephone)# exit

**Purpose**

Exits ephone configuration mode.
Verifying Telephony-Service Security Parameters

Step 1  Use the `show telephony-service security-info` command to display the security-related information that is configured in telephony-service configuration mode.

Step 2  Use the `show capf-server auth-string` command to display authentication strings for phones.

Step 3  Use the `show running-config` command to display the running configuration to verify telephony and per-phone security configuration.

Examples

The following example configures Cisco Unified CME security parameters.

```
telephony-service
  device-security-mode authenticated
  secure-signaling trustpoint cme-sccp
tftp-server-credentials trustpoint cme-tftp
load-cfg-file slot0:Ringlist.xml alias Ringlist.xml sign create
ephone 24
  device-security-mode authenticated
capf-auth-str 2734
cert-oper upgrade auth-mode auth-string
```

The following example shows two ways to display the telephony-service security settings.

```
Router# show telephony-service security-info
Skinny Server Trustpoint for TLS: cme-sccp
TFTP Credentials Trustpoint: cme-tftp
Server Security Mode: Secure
Global Device Security Mode: Authenticated

Router# show running-config
```

```
telephony-service
  secure-signaling trustpoint cme-sccp
  server-security-mode secure
device-security-mode authenticated
tftp-server-credentials trustpoint cme-tftp
```

The following example output displays configured strings (PINs) that users enter at the phone to establish CAPF authentication:

```
Router# show capf-server auth-string
```

```
<table>
<thead>
<tr>
<th>Mac-Addr</th>
<th>Auth-String</th>
</tr>
</thead>
<tbody>
<tr>
<td>000CCE3A817C</td>
<td>2734</td>
</tr>
<tr>
<td>001121116BDD</td>
<td>922</td>
</tr>
<tr>
<td>000D299D50DF</td>
<td>9182</td>
</tr>
<tr>
<td>000E7B10DAC</td>
<td>3114</td>
</tr>
<tr>
<td>000F90485077</td>
<td>3328</td>
</tr>
<tr>
<td>0013C352E7F1</td>
<td>0678</td>
</tr>
</tbody>
</table>
```
Configuring the CTL Client and CTL Provider

This procedure provides the CTL client with the names of the trustpoints it needs for the CTL file. The CTL client generates the CTL file. The CTL provider securely communicates the credentials of the Cisco Unified CME server functions to the CTL client that is running on another router.

The CTL client can run on the same router as Cisco Unified CME or on another, standalone router. When the CTL client runs on a standalone router (not a Cisco Unified CME router), you must configure a CTL provider on each Cisco Unified CME router.

When the CTL client is running on either a primary or secondary Cisco Unified CME router, you must configure a CTL provider on the other Cisco Unified CME router.

The CTL protocol is used to communicate between the CTL client and a CTL provider. Use of the CTL protocol ensures that the credentials of all Cisco Unified CME routers are present in the CTL file and that all Cisco Unified CME routers have access to the phone certificates that were issued by the CA. Both elements are prerequisites to secure communications.

The tasks to configure the CTL client and CTL providers differ slightly depending on whether the CTL client is running on a router that is also running Cisco Unified CME. Choose the appropriate procedure based on your network:

- CTL Client on a Cisco Unified CME Router
- CTL Client on a Router Other Than a Cisco Unified CME Router

### CTL Client on a Cisco Unified CME Router

2. On each remote Cisco Unified CME router (each Cisco Unified CME router on which the CTL client is not running): Configuring a CTL Provider on a Cisco Unified CME Router, page 185.

### CTL Client on a Router Other Than a Cisco Unified CME Router

Complete the following tasks when the CTL client runs on a router that is not running Cisco Unified CME:

1. On the router to receive the CTL client: Configuring a CTL Client on a Router Other Than a Cisco Unified CME Router, page 182

### Configuring a CTL Client on a Cisco Unified CME Router

Use the commands in this section to configure a CTL client on a Cisco Unified CME router.

If you have primary and secondary Cisco Unified CME routers, you can configure the CTL client on either one of them. When you have more than one Cisco Unified CME router in your network, you must also configure a CTL provider on each Cisco Unified CME router that is not running the CTL client, using the commands in the “Configuring a CTL Provider on a Cisco Unified CME Router” section on page 185.
### SUMMARY STEPS

1. enable
2. configure terminal
3. ctl-client
4. sast1 trustpoint trustpoint-label
5. sast2 trustpoint trustpoint-label
6. server {capf | cme | cme-tftp | tftp} ip-address trustpoint trustpoint-label
7. server cme ip-address username string password 0 string
8. regenerate
9. exit

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
  • Enter your password if prompted. |
| **Example:**  
  Router> enable | |

| **Step 2** configure terminal | Enters global configuration mode. |
| **Example:**  
  Router# configure terminal | |

| **Step 3** ctl-client | Enters CTL-client configuration mode. |
| **Example:**  
  Router(config)# ctl-client | |

| **Step 4** sast1 trustpoint label | Configures credentials for the primary SAST.  
  • label—SAST1 trustpoint name.  
  **Note** SAST1 and SAST2 certificates must be different from each other. The CTL file is always signed by SAST1. The SAST2 credentials are included in the CTL file, so that if the SAST1 certificate is compromised, the file can be signed by SAST2 to prevent phones from being reset to factory default. |
| **Example:**  
  Router(config-ctl-client)# sast1 trustpoint sast1tp | |

| **Step 5** sast2 trustpoint label | Configures credentials for the secondary SAST.  
  • label—SAST2 trustpoint name.  
  **Note** SAST1 and SAST2 certificates must be different from each other. The CTL file is always signed by SAST1. The SAST2 credentials are included in the CTL file, so that if the SAST1 certificate is compromised, the file can be signed by SAST2 to prevent phones from being reset to factory default. |
| **Example:**  
  Router(config-ctl-client)# sast2 trustpoint | |
### Command or Action

**Step 6**

```
server {capf | cme | cme-tftp | tftp} ip-address trustpoint trustpoint-label
```

**Example:**
```bash
Router(config-ctl-client)# server capf 10.2.2.2 trustpoint capftp
```

Configures a trustpoint for each server function that is running locally on the Cisco Unified CME router.

**Note**
Repeat this command with the appropriate keyword for each function that is running locally on the Cisco Unified CME router.

- **capf**—CAPF server.
- **cme**—Cisco Unified CME router.
- **cme-tftp**—Combined Cisco Unified CME router and TFTP server.
- **tftp**—TFTP server.
- **ip-address**—IP address of the Cisco Unified CME router. If there are multiple network interfaces, use the interface address in the local LAN to which the phones are connected.
- **trustpoint trustpoint-label**—Name of the PKI trustpoint for the entity.

**Step 7**

```
server cme ip-address username name-string password (0 | 1) password-string
```

**Example:**
```bash
Router(config-ctl-client)# server cme 10.2.2.2 username user3 password 0 38h2KL
```

(Optional) Provides information about another Cisco Unified CME router (primary or secondary) in the network, if one exists.

- **ip-address**—IP address of the other Cisco Unified CME router.
- **username name-string**—User name that is configured on the CTL provider.
- **password**—Encryption status of the password string.
  - 0—Not encrypted.
  - 1—Encrypted using Message Digest 5 (MD5).

**Note**
This option refers to the way that you want the password to appear in show command output and not to the way that you enter the password in this command.

- **password-string**—Administrative password of the CTL provider running on the remote Cisco Unified CME router.

**Step 8**

```
regenerate
```

**Example:**
```bash
Router(config-ctl-client)# regenerate
```

Creates a new CTLFile.tlv after you have made changes to the CTL client configuration.

**Step 9**

```
exit
```

**Example:**
```bash
Router(config-ctl-client)# exit
```

Exits CTL-client configuration mode.
Verifying a CTL Client

**Step 1**  
Use the `show ctl-client` command to display the CTL client configuration.

Examples

The following example configures a CTL client on the primary Cisco Unified CME router.

```
Router(config)# ctl-client
Router(config-ctl-client)# server capf 10.1.1.1 trustpoint cmeserver
Router(config-ctl-client)# server cme 10.1.1.1 trustpoint cmeserver
Router(config-ctl-client)# server tftp 10.1.1.1 trustpoint cmeserver
Router(config-ctl-client)# sast1 trustpoint cmeserver
Router(config-ctl-client)# sast2 trustpoint sast2
Router(config-ctl-client)# regenerate
```

The following example output from the `show ctl-client` command displays the trustpoints in the system.

```
Router# show ctl-client

CTL Client Information
------------------------
SAST 1 Certificate Trustpoint: cmeserver
SAST 1 Certificate Trustpoint: sast2
List of Trusted Servers in the CTL
  CME     10.1.1.1        cmeserver
  TFTP    10.1.1.1        cmeserver
  CAPF    10.1.1.1        cmeserver
```

Configuring a CTL Client on a Router Other Than a Cisco Unified CME Router

Use the commands in this section to configure a CTL client on an external router that is not a Cisco Unified CME router.

Additionally, you must configure a CTL provider on each Cisco Unified CME router, as explained in the “Configuring a CTL Provider on a Cisco Unified CME Router” section on page 185.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `ctl-client`
4. `sast1 trustpoint trustpoint-label`
5. `sast2 trustpoint trustpoint-label`
6. `server cme ip-address username name-string password {0 | 1} password-string`
7. `regenerate`
8. `exit`
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**        | **enable**<br>Enables privileged EXEC mode.  
  - Enter your password if prompted.  |
| **Example:**      | Router> enable |
| **Step 2**        | **configure terminal**<br>Enters global configuration mode.  |
| **Example:**      | Router# configure terminal |
| **Step 3**        | **ctl-client**<br>Enters CTL-client configuration mode.  |
| **Example:**      | Router(config)# ctl-client |
| **Step 4**        | **sast1 trustpoint label**<br>Configures credentials for the primary SAST.  
  - *label*—SAST1 trustpoint name.  
  **Note** SAST1 and SAST2 certificates must be different from each other, but either of them may use the same certificate as the Cisco Unified CME router to conserve memory. The CTL file is always signed by SAST1. The SAST2 credentials are included in the CTL file, so that if the SAST1 certificate is compromised, the file can be signed by SAST2 to prevent phones from being reset to factory default.  |
| **Example:**      | Router(config-ctl-client)# sast1 trustpoint sast1tp |
| **Step 5**        | **sast2 trustpoint label**<br>Configures credentials for the secondary SAST.  
  - *label*—SAST2 trustpoint name.  
  **Note** SAST1 and SAST2 certificates must be different from each other, but either of them may use the same certificate as the Cisco Unified CME router to conserve memory. The CTL file is always signed by SAST1. The SAST2 credentials are included in the CTL file, so that if the SAST1 certificate is compromised, the file can be signed by SAST2 to prevent phones from being reset to factory default.  |
| **Example:**      | Router(config-ctl-client)# sast2 trustpoint |
Configuring Phone Authentication

Step 1

Use the `show ctl-client` command to display the CTL client configuration.

Examples

The following example configures a CTL client on an external router that is not a Cisco Unified CME router.

Router(config)# ctl-client
Router(config-ctl-client)# sast1 trustpoint sast1
Router(config-ctl-client)# sast2 trustpoint sast2
Router(config-ctl-client)# server cme 172.19.245.1 username user4 password 0 c89L8o
Router(config-ctl-client)# regenerate
Router(config-ctl-client)# exit

Verifying a CTL Client

Step 1

Use the `show ctl-client` command to display the CTL client configuration.

Examples

The following example configures a CTL client on an external router that is not a Cisco Unified CME router.

Router(config)# ctl-client
Router(config-ctl-client)# sast1 trustpoint sast1
Router(config-ctl-client)# sast2 trustpoint sast2
Router(config-ctl-client)# server cme 172.19.245.1 username user4 password 0 c89L8o
Router(config-ctl-client)# regenerate
Router(config-ctl-client)# exit
The following sample output from the show ctl-client command displays the trustpoints in the system.

Router# show ctl-client

CTL Client Information
-----------------------------
SAST 1 Certificate Trustpoint: cmeserver
SAST 1 Certificate Trustpoint: sast2
List of Trusted Servers in the CTL
  CME     10.1.1.1        cmeserver
  TFTP    10.1.1.1        cmeserver
  CAPF    10.1.1.1        cmeserver

Configuring a CTL Provider on a Cisco Unified CME Router

When you have more than one Cisco Unified CME router in your network, use the commands in this section to establish a CTL provider on each Cisco Unified CME router on which the CTL client is not running.

SUMMARY STEPS

1. enable
2. configure terminal
3. credentials
4. ip source-address ip-address port port-number
5. trustpoint trustpoint-label
6. ctl-service admin username secret {0 | 1} password-string
7. exit

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3 credentials</td>
<td>Enters credentials-interface mode to configure a CTL provider.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# credentials</td>
<td></td>
</tr>
</tbody>
</table>
### Command or Action

<table>
<thead>
<tr>
<th>Step 4</th>
<th>ip source-address [ip-address [port [port-number]]]</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>Example:</em></td>
<td>Router(config-credentials)# ip source-address 172.19.245.1 port 2444</td>
</tr>
</tbody>
</table>

**Purpose:** Identifies the local router on which this CTL provider is being configured.
- *ip-address*—Router IP address, typically one of the addresses of the Ethernet port of the router.
- *port port-number*—TCP port for credentials service communication. Default is 2444. You should use 2444.

<table>
<thead>
<tr>
<th>Step 5</th>
<th>trustpoint trustpoint-label</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>Example:</em></td>
<td>Router(config-credentials)# trustpoint ctlpv</td>
</tr>
</tbody>
</table>

**Purpose:** Configures the trustpoint to be used for TLS sessions with the CTL client.
- *trustpoint-label*—CTL provider trustpoint label.

| Step 6 | ctl-service admin username secret {0 | 1} password-string |
| --- | --- |
| *Example:* | Router(config-credentials)# ctl-service admin user4 secret 0 c89L8o |

**Purpose:** Specifies a user name and password to authenticate the CTL client when it connects to retrieve the credentials during the CTL protocol. You must use this command before you enable the CTL provider.
- *username*—Name that will be used to authenticate the client.
- *secret*—Character string for login authentication and whether the string should be encrypted when it is stored in the running configuration.
  - 0—Not encrypted.
  - 1—Encrypted using Message Digest 5 (MD5).
- *password-string*—Character string for login authentication.

<table>
<thead>
<tr>
<th>Step 7</th>
<th>exit</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>Example:</em></td>
<td>Router(config-credentials)# exit</td>
</tr>
</tbody>
</table>

**Purpose:** Exits credential configuration mode.

### Verifying a CTL Provider

**Step 1**
Use the `show credentials` command to display credentials settings.

### Examples

The following example sets up a CTL provider on a Cisco Unified CME router with the IP address 172.19.245.1.

```bash
Router(config)# credentials
Router(config-credentials)# ip source-address 172.19.245.1 port 2444
Router(config-credentials)# trustpoint ctlpv
Router(config-credentials)# ctl-service admin user4 secret 0 c89L8o
```
The following is sample output from the `show credentials` command:

```bash
Router# show credentials
Credentials IP: 172.19.245.1
Credentials PORT: 2444
Trustpoint: ctlpv
```

### Configuring the CAPF Server

This task configures the CAPF server on the Cisco Unified CME router. A certificate must be provisioned for the CAPF server so that it can establish a TLS session with the phone during certificate operation.

The CAPF server can install, fetch, or delete locally significant certificates (LSCs) on security-enabled phones.

**Note**
When you use the CAPF server to install phone certificates, arrange to do so during a scheduled maintenance window. The generation of many certificates at the same time may cause call-processing interruptions.

**Note**
If you select the authentication-string method of authentication in the `auth-mode` command, you must also enter an authentication string on each phone that is receiving an updated LSC. For instructions on this task, see the “Entering the Authentication String on the Phone” section on page 191.

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `capf-server`
4. `trustpoint-label label`
5. `cert-enroll-trustpoint label password {0 | 1} password-string`
6. `source-addr ip-address`
7. `port tcp-port`
8. `auth-mode {auth-string | LSC | MIC | none | null-string}`
9. `auth-string {delete | generate} {all |ephone-tag} [auth-string]`
10. `phone-key-size {512 | 1024 | 2048}`
11. `keygen-retry number`
12. `keygen-timeout minutes`
13. `cert-oper {delete all | fetch all | upgrade all}`
14. `exit`
## DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> capf-server</td>
<td>Enters CAPF-server configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> trustpoint-label label</td>
<td>Specifies the label of the trustpoint whose certificate is to be used for TLS connection between the CAPF server and the phone.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 5</strong> cert-enroll-trustpoint trustpoint-label password (0</td>
<td>1) password-string</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 6</strong> source-addr ip-address</td>
<td>Defines the IP address of the CAPF server on the Cisco Unified CME router.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 7</strong> port tcp-port</td>
<td>(Optional) Defines the TCP port number on which the CAPF server listens for socket connections from the phones.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Enter your password if prompted.</td>
</tr>
</tbody>
</table>
### Command or Action

**Step 8**

```
auth-mode {auth-string | LSC | MIC | none | null-string}
```

**Example:**

Router(config-capf-server)# auth-mode auth-string

**Purpose**

Specifies the type of authentication to use during CAPF sessions to verify endpoints that request certificates.

- **auth-string**—The phone user enters a special authentication string at the phone. The string is provided to the user by the system administrator and is configured using the `auth-string generate` command.
- **LSC**—The phone provides its LSC for authentication, if one exists.
- **MIC**—The phone provides its MIC for authentication, if one exists. If this option is chosen, the MIC’s issuer certificate must be imported into a PKI trustpoint. See the “Manually Importing MIC Root Certificate on the Cisco Unified CME Router” section on page 168.
- **none**—No certificate upgrade is initiated. This is the default.
- **null-string**—No authentication.

**Step 9**

```
auth-string {delete | generate} {all | ephone-tag} [digit-string]
```

**Example:**

Router(config-capf-server)# auth-string generate all

**Purpose**

(Optional) Creates or removes authentication strings for all the secure ephones or for specified secure ephones. Use this command if the `auth-string` keyword is specified in the `auth-mode` command. Strings become part of the ephone configuration. Use the `show capf-server auth-string` command to view authentication strings.

- **delete**—Remove authentication strings for the specified secure devices.
- **generate**—Create authentication strings for the specified secure devices.
- **all**—All phones.
- **ephone-tag**—Identifier for the ephone to receive the authentication string.
- **digit-string**—String of digits that the phone user must dial for CAPF authentication. The string can be from 4 to 10 digits. If this value is not specified, a random string is generated for each phone. For instructions on how to enter the string from the phone, see the “Entering the Authentication String on the Phone” section on page 191.

**Note**

You can also define an authentication string for an individual ephone using the `capf-auth-str` command.

**Step 10**

```
phone-key-size (512 | 1024 | 2048)
```

**Example:**

Router(config-capf-server)# phone-key-size 2048

**Purpose**

(Optional) Specifies the size of the RSA key pair that is generated on the phone for the phone’s certificate, in bits.

- **512**—512.
- **1024**—1024. This is the default.
- **2048**—2048.
Configuring Phone Authentication

Step 1

Use the `show capf-server summary` command to display CAPF-server configuration information.

Examples

The following example sets up a CAPF server.

```
Router(config)# capf-server
Router(config-capf-server)# source addr 10.10.10.1
Router(config-capf-server)# trustpoint-label tp1
Router(config-capf-server)# cert-oper upgrade all
Router(config-capf-server)# cert-enroll-trustpoint ra1 password 0 x8oWiet
Router(config-capf-server)# auth-mode auth-string
Router(config-capf-server)# auth-string generate all
Router(config-capf-server)# port 3804
Router(config-capf-server)# phone-key-size 1024
```

The following sample output displays CAPF-server parameters.

```
Router# show capf-server summary

CAPF Server Configuration Details
```

Verifying the CAPF Server

Step 1

(Optional) Specifies the number of times that the server sends a key generation request.

- **number**—Number of retries. Range is from 0 to 100. Default is 3.

Step 12

(Optional) Specifies the amount of time that the server waits for a key generation response from the phone, in minutes.

- **minutes**—Number of minutes before the generation process times out. Range is from 1 to 120. Default is 30.

Step 13

Step 14

Exits CAPF-server configuration mode.

Note

You can use the `cert-oper` command in ephone configuration mode for certificate operations on individual ephones. See the “Configuring Telephony-Service Security Parameters” section on page 173.
Trustpoint for TLS With Phone: tp1
Trustpoint for CA operation: ra1
Source Address: 10.10.10.1
Listening Port: 3804
Phone Key Size: 1024
Phone KeyGen Retries: 3
Phone KeyGen Timeout: 30 minutes

The following example output displays configured strings (PINs) that users enter at the phone to establish CAPF authentication:

```
Router# show capf-server auth-string
```

<table>
<thead>
<tr>
<th>Mac-Addr</th>
<th>Auth-String</th>
</tr>
</thead>
<tbody>
<tr>
<td>000CCE3A817C</td>
<td>7012</td>
</tr>
<tr>
<td>001121116BDD</td>
<td>922</td>
</tr>
<tr>
<td>000D299D50DF</td>
<td>9182</td>
</tr>
<tr>
<td>000ED7B10DAC</td>
<td>3114</td>
</tr>
<tr>
<td>000F90485077</td>
<td>3328</td>
</tr>
<tr>
<td>0013C352E7F1</td>
<td>0678</td>
</tr>
</tbody>
</table>

### Entering the Authentication String on the Phone

This task is optional. It is required only for the one-time installation of an LSC on a phone and only if you specify the authentication string method of authentication.

If you use the `auth-string` keyword with the `auth-mode` command in CAPF-server configuration mode or the `cert-oper` command in ephone configuration mode, an authentication string must be entered on a phone before the phone’s LSC can be installed. The authentication string itself is defined using the `auth-string` command in CAPF-server configuration mode or the `capf-auth-str` command in ephone configuration mode. The authentication string must be communicated to the phone user so that it can be entered on the phone before the LSC is installed.

The phone user can perform the following procedure to install the certificate. The authentication string applies for one-time use only.

**Note**

You can list authentication strings for phones by using the `show capf-server auth-string` command.

### Prerequisites

- Verify that the CAPF certificate exists in the CTL file.
- Verify that a signed image exists on the phone; refer to the Cisco Unified IP phone administration documentation that supports your phone model.
- Verify that the device has registered.
- Verify that the device security mode is nonsecure.

### SUMMARY STEPS

1. Press the Settings button.
2. If the configuration is locked, press **# (asterisk, asterisk, pound sign) to unlock it.
5. When prompted for the authentication string, enter the string provided by the system administrator and press the Submit soft key.

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Press the Settings button.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>If the configuration is locked, press **# (asterisk, asterisk, pound sign) to unlock it.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Scroll down the Settings menu. Highlight Security Configuration and press the Select soft key.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Scroll down the Security Configuration menu. Highlight LSC and press the Update soft key.</td>
</tr>
<tr>
<td>Step 5</td>
<td>When prompted for the authentication string, enter the string provided by the system administrator and press the Submit soft key.</td>
</tr>
</tbody>
</table>

The phone installs, updates, deletes, or fetches the certificate, depending on the current CAPF configuration.

You can monitor the progress of the certificate operation by viewing the messages that display on the phone. After you press Submit, the message “Pending” displays under the LSC option. The phone generates the public and private key pair and displays the information on the phone. When the phone successfully completes the process, the phone displays a successful message. If the phone displays a failure message, you entered the wrong authentication string or did not enable the phone for upgrade.

At any time, you can stop the process by choosing the Stop option.

You can verify that the certificate installed on the phone by choosing Settings > Model Information and viewing the LSC setting, which indicates Installed or Not Installed.

### Examples

The following example shows the running configuration for a Cisco Unified CME system that has been configured with Cisco Unified CME phone authentication. It has three components:

- Configuration of Cisco IOS CA Server: Example
- Configuration of Secure CME Router: Example
- Configuration of CTL Client Running on Another Router: Example

#### Configuration of Cisco IOS CA Server: Example

```plaintext
! crypto pki server iosca
grant auto

database url flash:
!
crypto pki trustpoint iosca
revocation-check none
rsakeypair iosca
!
crypto pki certificate chain iosca
certificate ca 01
308201F9 30820162 ...
```
Configuration of Secure CME Router: Example

! ip dhcp pool cme-pool
    network 10.1.1.0 255.255.255.0
    option 150 ip 10.1.1.1
    default-router 10.1.1.1

! capf-server
    port 3804
    auth-mode null-string
    cert-enroll-trustpoint iosra password 1 00071A1507545A545C
    trustpoint-label cmeserver
    source-addr 10.1.1.1

! crypto pki server iosra
    grant auto
    mode ra
    database url slot0:

! crypto pki trustpoint cmeserver
    enrollment url http://10.1.1.100:80
    serial-number
    revocation-check none
    rsakeypair cmeserver

! crypto pki trustpoint sast2
    enrollment url http://10.1.1.100:80
    serial-number
    revocation-check none
    rsakeypair sast2

! crypto pki trustpoint iosra
    enrollment url http://10.1.1.200:80
    revocation-check none
    rsakeypair iosra

! crypto pki certificate chain cmeserver
    certificate 1B
    30820207 30820170 A0030201 0202011B 300D0609 2A864886 F70D0101 04050030 ....
     quit
    certificate ca 01
    3082026B 308201D4 A0030201 02020101 300D0609 2A864886 F70D0101 04050030 ...
     quit
    crypto pki certificate chain sast2
    certificate 1C
    30820207 30820170 A0030201 0202011C 300D0609 2A864886 F70D0101 04050030 ....
     quit
    certificate ca 01
    3082026B 308201D4 A0030201 02020101 300D0609 2A864886 F70D0101 04050030 ....
     quit
    crypto pki certificate chain capf-tp
    crypto pki certificate chain iosra
    certificate 04
    30820201 3082016A A0030201 02020104 300D0609 2A864886 F70D0101 04050030 ....
     certificate ca 01
    308201F9 30820162 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
....
quits
!
!
credentials
crl-service admin cisco secret 1 094F471A1A0A464058
ip source-address 10.1.1.1 port 2444
trustpoint cmeserver
!
!
teledphony-service
no auto-reg-ephone
load 7960-7940 P00307010200
load 7914 S00104000100
load 7941GE TERM41.7-0-0-129DEV
load 7970 TERM70.7-0-0-77DEV
max-ephones 20
max-dn 10
ip source-address 10.1.1.1 port 2000 secondary 10.1.1.100
secure-signaling trustpoint cmeserver
cnf-file location flash:
cnf-file perphone
dialplan-pattern 1 2... extension-length 4
max-conferences 8 gain -6
transfer-pattern ....
tftp-server-credentials trustpoint cmeserver
server-security-mode secure
device-security-mode encrypted
load-cfg-file slot0:Ringlist.xml alias Ringlist.xml sign
load-cfg-file slot0:P00307010200.bin alias P00307010200.bin
load-cfg-file slot0:P00307010200.loads alias P00307010200.loads
load-cfg-file slot0:P00307010200.sb2 alias P00307010200.sb2
load-cfg-file slot0:P00307010200.sbn alias P00307010200.sbn
load-cfg-file slot0:cn41.2-7-4-116dev.sbn alias cn41.2-7-4-116dev.sbn
load-cfg-file slot0:Jar41.2-9-0-101dev.sbn alias Jar41.2-9-0-101dev.sbn
load-cfg-file slot0:CVM41.2-0-0-96dev.sbn alias CVM41.2-0-0-96dev.sbn
load-cfg-file slot0:CVM41.DEFAUL.load alias CVM41.DEFAUL.load
load-cfg-file slot0:TERM70.DEFAUL.load alias TERM70.DEFAUL.load
load-cfg-file slot0:Jar70.2-9-0-54dev.sbn alias Jar70.2-9-0-54dev.sbn
load-cfg-file slot0:cn70.2-7-4-58dev.sbn alias cn70.2-7-4-58dev.sbn
load-cfg-file slot0:CVM70.2-0-0-49dev.sbn alias CVM70.2-0-0-49dev.sbn
load-cfg-file slot0:DistinctiveRingList.xml alias DistinctiveRingList.xml sign
load-cfg-file slot0:Plan01.raw alias Plan01.raw sign
load-cfg-file slot0:S00104000100.sbn alias S00104000100.sbn
!
!
ephone 1
device-security-mode encrypted
cert-oper upgrade auth-mode null-string
mac-address 000C.CE3A.817C
type 7960 addon 1 7914
button 1:2 8:8
!
!
ephone 2
device-security-mode encrypted
capf-auth-str 2476
cert-oper upgrade auth-mode null-string
mac-address 0011.2111.6BD

type 7970
button 1:1
Configuration of CTL Client Running on Another Router: Example

```
ctl-client
server cme 10.1.1.100 trustpoint cmeserver
server cme 10.1.1.1 username cisco password 1 0822455D0A16544541
sast1 trustpoint cmeserver
sast2 trustpoint sast1
```

Feature History for Phone Authentication

<table>
<thead>
<tr>
<th>Cisco Unified CME Version</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.0</td>
<td>Phone authentication for Cisco Unified CME phones was introduced.</td>
</tr>
</tbody>
</table>
Related Features

PKI Management
Cisco IOS public key infrastructure (PKI) provides certificate management to support security protocols such as IP Security (IPSec), secure shell (SSH), and secure socket layer (SSL). For more information, see the following documents:

- “Part 5: Implementing and Managing a PKI” in the Cisco IOS Security Configuration Guide, Release 12.4
- Cisco IOS Security Command Reference, Release 12.4

Glossary

**authentication**—Process that verifies the identity of an entity.

**CA**—Certification authority. Service that is responsible for managing certificate requests and issuing certificates to participating IPSec network devices. This service provides centralized key management for participating devices and is explicitly trusted by the receiver to validate identities and to create digital certificates.

**CAPF**—Certification authority proxy function. Process whereby supported devices can request locally significant certificates.

**certificate**—Electronic document that binds a user's or device's name to its public key. Certificates are commonly used to validate digital signatures.

**CRL**—Certificate revocation list. Electronic document that contains a list of revoked certificates. The CRL is created and digitally signed by the CA that originally issued the certificates. The CRL contains dates for when the certificate was issued and when it expires. A new CRL is issued when the current CRL expires.

**CTL**—Certificate trust list. Digitally signed configuration file that contains a predefined list of trusted items that the Cisco system administrators security token (SAST or security token) signs, using the router’s private key. This file provides authentication information to validate the certificates for servers and security tokens for Cisco Unified IP phones. Its filename format is SEP<mac-addr>.cnf.xml.sgn.

**encryption**—Process that ensures that only the intended recipient receives and reads the data; process that ensures the confidentiality of the information; process that translates data into ciphertext, which appears random and meaningless.

**file authentication**—Process that validates digitally signed files that the phone downloads. The phone validates the signature to make sure that file tampering did not occur after the file creation.

**LSC**—Locally significant certificate. Certificate issued to a supported phone through a CAPF from a true CA. With certain phone models, one LSC and one MIC can exist in the same phone, in which case the LSC takes precedence over the MIC for authentication to the Cisco Unified CME after you configure the device security mode for authentication.

**MIC**—Manufacture installed certificate. Cisco manufacturing automatically installs this certificate in supported phone models. With certain phone models, one MIC and one LSC can exist in the same phone, in which case the LSC takes precedence over the MIC for authentication to the Cisco Unified CME after you configure the device security mode for authentication. You cannot overwrite or delete the MIC.

**peer certificate**—Certificate presented by a peer, which contains the peer's public key and is signed by the trustpoint CA.
**PKI**—Cisco IOS public key infrastructure (PKI) provides certificate management to support security protocols such as IP Security (IPSec), secure shell (SSH), and secure socket layer (SSL). System that manages encryption keys and identity information for components of a network that participate in secured communications.

**RA**—Registration authority. Server that acts as a proxy for the CA so that CA functions can continue when the CA is offline. Although the RA is often part of the CA server, the RA can also be an additional application, requiring an additional device to run it.

**RSA**—Public-key cryptographic system that can be used for encryption and authentication. The acronym stands for Ron Rivest, Adi Shamir, and Leonard Adleman, the inventors of the technique.

**RSA keys**—A key is a series of characters used for encryption and decryption. An RSA key pair contains a public and a private key. An RSA key pair is required before you can obtain a certificate for your router.

**SAST**—System administrator security token. A certificate and public-private key pair that is used by the CTL client to generate or regenerate the CTL file. There are two SASTs, called SAST1 and SAST2, which use two different certificates. If the certificate for the first one is lost or compromised, the CTL client uses the certificate of the second one to regenerate the CTL file.

**TLS**—Transport Layer Security. An IETF-defined security protocol (RFP 2246) that provides integrity, authentication, and encryption. TLS resides in the TCP layer in the IP communications stack.

**trustpoint**—Location that stores digitally signed certificates.
Transcoding Support

This module describes how to set up transcoding between G.729 voice signals and G.711 for various Cisco Unified CallManager Express (Cisco Unified) CME features. It includes the following sections:

- Transcoding Support Overview, page 199
- Configuring Transcoding Support, page 201
- Verifying Transcoding Support, page 215
- Examples, page 215
- Troubleshooting Transcoding Support, page 217
- Feature History for Transcoding Support, page 221
- Related Features, page 221

Note


Transcoding Support Overview

Note

For a summary of the functionality introduced in different releases, see the “Feature History for Transcoding Support” section on page 221.

Versions of Cisco Unified CME prior to Cisco CME 3.2 supported G.729 compressed voice calls for two-party calls only. Cisco CME 3.2 and later versions support transcoding between G.711 and G.729 for the following features:

- Ad hoc conferencing—One or more remote conferencing parties uses G.729.
- Call transfer and forward—One leg of a Voice over IP (VoIP)-to-VoIP hairpin call uses G.711 and the other leg uses G.729. A hairpin call is an incoming call that is transferred or forwarded over the same interface from which it arrived. As shown in Figure 16, the interface could be a Cisco 2800 router.
- Cisco Unity Express—An H.323 or SIP call using G.729 is forwarded to Cisco Unity Express. Note that Cisco Unity Express supports only G.711, so G.729 must be transcoded.
Transcoding Support Overview

Music on hold (MOH)—The phone receiving MOH is part of a system that uses G.729. The G.711 MOH is translated to G.729. Because of compression, the MOH sent using G.729 loses the fidelity that it has with G.711.

Figure 16 provides an example of each of the four call situations described.

Figure 16 Three-Way Conferencing, Call Transfer and Forward, Cisco Unity Express, and MOH Between G.711 and G.729

A situation in which transcoding resources may be used is when you use the codec command to select the G.729r8 codec to help save network bandwidth for a remote IP phone. If a Cisco Unified CME conference is initiated, all phones in the conference switch to G.711 mu-law. To allow the phone to retain its G.729r8 codec setting even when being joined to a conference, you can use the dspfarm-assist keyword with the codec command to specify that this phone’s calls should use the resources of a configured DSP farm for transcoding. For example, there are two remote phones (A and B) and a local phone (C) that initiates a conference with them. Both A and B are configured to use the G.729r8 codec with the assistance of the DSP-farm transcoder. In the conference, the call leg from C to the conference uses the G.711 mu-law codec, and the call legs from A and B to the Cisco Unified CME router use the G.729r8 codec.

You should consider your options carefully when deciding to use the dspfarm-assist keyword with the codec command. The benefit is that it allows calls to use the G.729r8 codec on the call leg between the IP phone and the Cisco Unified CME router, which saves network bandwidth. The disadvantage is that for situations requiring G.711 codecs, such as conferencing and Cisco Unity Express, DSP resources that are possibly scarce will be used to transcode the call, and delay will be introduced while voice is shuttled to and from the DSP. In addition, the overuse of this feature can mask configuration errors in the codec selection mechanisms involving dial peers and codec lists.

Therefore, it is recommended that the dspfarm-assist keyword be used sparingly and only when absolutely required for bandwidth savings or when you know the phone will be participating very little, if at all, in calls that require a G.711 codec.
If the `dspfarm-assist` keyword has been configured for a phone and a DSP resource is not available when needed for transcoding, a phone registered to the local Cisco Unified CME router will use G.711 instead of G.729r8. This is not true for non-SCCP call legs; if DSP resources are not available for the transcoding required for a conference, for example, the conference will not be created.

**Prerequisites**

- Cisco Unified CME routers and external voice routers on the same LAN must be configured with digital signal processors (DSPs) that support transcoding.
- For Cisco CME 3.2 and later versions, DSPs on the NM-HDV, NM-HDV2, NM-HD-1V, NM-HD-2V and NM-HD-2VE can be configured for transcoding. PVDM2-xx on the Cisco 2800 series and the Cisco 3800 series motherboards can also be configured for transcoding.

**Restrictions**

Transcoding between G.711 and G.729 does not support the following:

- Meet-me conferencing
- Multiple-party conferencing
- Transcoding security

**Configuring Transcoding Support**

Regardless of whether you are planning to use transcoding for all or some of the conferencing, call transfer, call forward, Cisco Unity Express, and MOH functionalities, one configuration is required for all. The configuration tasks are as follows:

- Determining Digital Signal Processor Resources, page 201
- Determining the Correct DSP Allocation for Transcoding, page 205
- Provisioning NMs or NM Farms for Transcoding, page 205
- Setting Up DSP Farms for NMs, page 205
- Changing the Number of Transcoding Sessions, page 212 (Optional)
- Configuring Cisco Unified CME to Act as the DSP Farm Host, page 213

**Determining Digital Signal Processor Resources**

Transcoding is facilitated through DSPs, which are located in network modules (NMs). All NMs have single in-line memory module (SIMM) sockets or packet voice/data modules (PVDM) slots that each hold a Packet Voice DSP Module (PVDM). Each PVDM holds DSPs. As shown in Figure 17, the NM-HDV has five SIMM sockets or PVDM slots that each hold a 12-Channel PVDM (PVDM-12). Each PVDM-12 holds three TI 549 DSPs. Each DSP supports four channels.
A router can have multiple NMs. A group of NMs is called an *NM farm*. Figure 18 shows an NM farm for the NM-HDV.
DSP resources can be used to provide voice termination of the digital voice trunk group or resources for the DSP farm. The collection of DSP resources available for transcoding and not used for voice termination is called a DSP farm. See Figure 19. The DSP farm is managed by Cisco Unified CME.

Transcoding of G.729 calls to G.711 allows G.729 calls to participate in existing G.711 software-based, three-party conferencing, thus eliminating the need to divide DSPs between transcoding and conferencing.
To determine how many DSP voice resources are on your Cisco Unified CME router, use the `show voice dsp` command.

To determine how many DSP farms have been configured, use the `show sdspfarm sessions` and `show sdspfarm units` commands.
Determining the Correct DSP Allocation for Transcoding

You must allocate the DSP resources that are used by NMs or NM farms to either a DSP farm or the system’s digital voice trunk group that handles standard voice termination. For information about determining if your router has the correct DSP allocation for transcoding, refer to the “Allocation of DSP Resources” section in the “Configuring Enhanced Conferencing and Transcoding for Voice Gateway Routers” chapter of the Cisco CallManager and Cisco IOS Interoperability Guide.

Provisioning NMs or NM Farms for Transcoding

To provision NMs or NM farms for transcoding, you must determine the required number of PVDMs and install them in either NMs or NM farms. A single NM holds up to five PVDMs. On routers capable of holding multiple devices, NMs or NM farms can be allocated to support different functionalities.

---

**Step 1**
Determine performance requirements.

Determine the number of transcoding sessions that your router must support.

**Step 2**
Determine the number of DSPs that are required.

From Table 8 or Table 9 in the “Allocation of DSP Resources” section of the “Configuring Enhanced Conferencing and Transcoding for Voice Gateway Routers” chapter of the Cisco CallManager and Cisco IOS Interoperability Guide, determine the number of DSPs that are required to support the transcoding sessions. Note that Cisco Unified CME does not support DSP-farm conferencing, so only the transcoding portion of this discussion applies to Cisco Unified CME. If voice termination is required in addition, determine the additional number of required DSPs from the tables. For example, 16 transcoding sessions (30-ms packetization) and 4 G.711 voice calls require two DSPs.

**Step 3**
Determine the number of DSPs that are supportable.

From Table 4 in the “Allocation of DSP Resources” section of the “Configuring Enhanced Conferencing and Transcoding for Voice Gateway Routers” chapter of the Cisco CallManager and Cisco IOS Interoperability Guide, determine the maximum number of NMs or NM farms that your router can support.

**Step 4**
Verify your solution.

Ensure that your requirements fall within router capabilities, taking into account whether your router supports multiple NMs or NM farms. If necessary, reassess performance requirements.

**Step 5**
Install hardware to prepare your system for DSP-farm configuration.

Install PVDMs, NMs, and NM farms as needed.

---

Setting Up DSP Farms for NMs

DSP farm configuration instructions for the various NMs are described in the following sections:

- Setting Up DSP Farms for NM-HDVs, page 206
- Setting Up DSP Farms for NM-HDs and NM-HDV2s, page 207
Setting Up DSP Farms for NM-HDVs

Setting up DSP farms on NM-HDVs involves enabling DSP farms and Skinny Client Control Protocol (SCCP) on the Cisco Unified CME routers. You must also specify the number of transcoding sessions per DSP farm and select a local SCCP interface.

SUMMARY STEPS

1. enable
2. configure terminal
3. voice-card slot
4. dsp services dspfarm
5. exit
6. sccp local interface-type interface-number
7. sccp ccm ip-address priority priority-number
8. sccp
9. dspfarm transcoder maximum sessions number
10. dspfarm

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Router&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3 voice-card slot</td>
<td>Enters voice-card configuration mode and identifies the slot in the chassis in which the NM-HDV or NM-HDV farm is located.</td>
</tr>
<tr>
<td>Example: Router(config)# voice-card 1</td>
<td></td>
</tr>
<tr>
<td>Step 4 dsp services dspfarm</td>
<td>Enables DSP-farm services on the NM-HDV or NM-HDV farm.</td>
</tr>
<tr>
<td>Example: Router(config-voicecard)# dsp services dspfarm</td>
<td></td>
</tr>
<tr>
<td>Step 5 exit</td>
<td>Returns to global configuration mode.</td>
</tr>
<tr>
<td>Example: Router(config-voicecard)# exit</td>
<td></td>
</tr>
</tbody>
</table>
Configuring Transcoding Support

Setting Up DSP Farms for NM-HDs and NM-HDV2s

Setting up DSP farms on NM-HDs and NM-HDV2s involves enabling DSP farms and SCCP on routers. You must also select a local SCCP interface and configure a DSP farm profile and a Cisco Unified CME group. The DSP farm profile declares codec usage and the maximum number of transcoding sessions and associates SCCP with the DSP farm profile.

A Cisco Unified CME group is a naming device under which data for the DSP farms is declared. Only one group is required. For the Cisco Unified CME group you must assign a priority to the group, associate the group with a DSP farm profile, and set the keepalive, switchback, and switchover parameters.

### SUMMARY STEPS

1. enable
2. configure terminal

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 6</strong> <code>sccp local interface-type interface-number</code></td>
<td>Selects the local interface that the SCCP applications (transcoding and conferencing) should use to register with Cisco Unified CME.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# sccp local FastEthernet 0/0</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> <code>sccp ccm ip-address priority priority-number</code></td>
<td>Specifies the Cisco Unified CME address.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# sccp ccm 10.10.10.1 priority 1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong> <code>sccp</code></td>
<td>Enables SCCP and its associated transcoding and conferencing applications.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# sccp</td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong> <code>dspfarm transcoder maximum sessions number</code></td>
<td>Specifies the maximum number of transcoding sessions to be supported by the DSP farm. A DSP can support up to four transcoding sessions.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# dspfarm transcoder maximum sessions 12</td>
<td><strong>Note</strong> When you assign this value, take into account the number of DSPs allocated for conferencing services.</td>
</tr>
<tr>
<td><strong>Step 10</strong> <code>dspfarm</code></td>
<td>Enables the DSP farm.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# dspfarm</td>
<td></td>
</tr>
</tbody>
</table>
3. voice-card slot
4. dsp services dspfarm
5. exit
6. sccp local interface-type interface-number
7. sccp ccm ip-address identifier identifier-number
8. sccp
disp services dspfarm
9. sccp ccm group group-number
10. bind interface interface-type interface-number
11. associate ccm identifier-number priority
12. associate profile profile-identifier register device-name
13. keepalive retries number
14. switchover method {graceful | immediate}
15. switchback method {graceful | guard timeout-guard-value | immediate | uptime uptime-timeout-value}
16. switchback interval seconds
17. exit
disp services dspfarm profile profile-identifier transcode
18. codec codec-type
19. maximum sessions number
20. associate application sccp
21. exit
22. exit

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td>Enter your password if prompted.</td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3 voice-card slot</td>
<td>Enters voice-card configuration mode and identifies the slot in the</td>
</tr>
<tr>
<td>Example:</td>
<td>chassis in which the NM-HDV or NM-HDV farm is located.</td>
</tr>
<tr>
<td>Router(config)# voice-card 1</td>
<td></td>
</tr>
<tr>
<td>Step 4 dsp services dspfarm</td>
<td>Enables DSP-farm services on the NM-HDV or NM-HDV farm.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-voicecard)# dsp</td>
<td></td>
</tr>
<tr>
<td>services dspfarm</td>
<td></td>
</tr>
</tbody>
</table>
### Transcoding Support

**Configuring Transcoding Support**

#### Step 5

**Command or Action:**

```
exit
```

**Example:**

```
Router(config-voicecard)# exit
```

**Purpose:**

Exits voice-card configuration mode.

#### Step 6

**Command or Action:**

```
sc Snape local interface-type interface-number
```

**Example:**

```
Router(config)# sccp local FastEthernet 0/0
```

**Purpose:**

Selects the local interface that the SCCP applications (transcoding and conferencing) should use to register with Cisco Unified CME.

- **interface-type**—Interface type that the SCCP application uses to register with Cisco Unified CME. The type can be an interface address or a virtual-interface address such as Ethernet.
- **interface-number**—Interface number that the SCCP application uses to register with Cisco Unified CME.

#### Step 7

**Command or Action:**

```
sc cp ccm ip-address identifier
```

**Example:**

```
Router(config)# sccp ccm 10.10.10.1 priority 2
```

**Purpose:**

Specifies the Cisco Unified CME address.

- **ip-address**—IP address of the Cisco Unified CME server.
- **identifier**—Identifier used to associate the SCCP Cisco Unified CME IP address with a Cisco Unified CME group. See the `associate ccm` command in Step 11.

#### Step 8

**Command or Action:**

```
sccp
```

**Example:**

```
Router(config)# sccp
```

**Purpose:**

Enables SCCP and its associated transcoding and conferencing applications.

#### Step 9

**Command or Action:**

```
sc cp ccm group group-number
```

**Example:**

```
Router(config)# sccp ccm group 1
```

**Purpose:**

Creates a Cisco Unified CME group and enters the SCCP configuration mode for Cisco Unified CME.

- **group-number**—Number that identifies the Cisco Unified CME group. Range is 1 to 65535. There is no default value.

#### Step 10

**Command or Action:**

```
bind interface interface-type interface-number
```

**Example:**

```
Router(config-sccp-ccm)# bind interface FastEthernet 0/0
```

**Purpose:**

(Optional) Binds an interface to a Cisco Unified CME group so that the selected interface is used for all calls that belong to the profiles that are associated to this Cisco Unified CME group. This command is optional, but it is recommended if you have more than one profile or if you are on different subnets, to ensure that the correct interface is selected.
### Transcoding Support

#### Configuring Transcoding Support

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 11</strong> <code>associate ccm identifier-number priority</code></td>
<td>Associates a Cisco Unified CME with a Cisco Unified CME group and establishes its priority within the group.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-sccp-ccm)# associate ccm 1 priority</td>
</tr>
<tr>
<td></td>
<td>- <code>identifier-number</code>—Number that identifies Cisco Unified CME. Range is 1 to 65535. There is no default value.</td>
</tr>
<tr>
<td></td>
<td>- <code>priority</code>—The priority of the Cisco Unified CME router in the Cisco Unified CME group. The default is 1 because only one Cisco Unified CME group is possible.</td>
</tr>
</tbody>
</table>

| **Step 12** `associate profile profile-identifier register device-name` | Associates a DSP farm profile with a Cisco Unified CME group. |
| **Example:** | Router(config-sccp-ccm)# associate profile 1 register mtp000a8eaca80 |
| | - `profile-identifier`—Number that identifies the DSP farm profile. Range is 1 to 65535. There is no default value. |
| | - `register device-name`—User-specified device name in Cisco Unified CME. The `device-name` must use the format of `mtpmac-address`, where the `mac-address` is the burnt-in address (bia) of the physical interface that is used to register as the SCCP device. |

| **Step 13** `keepalive retries number` | Sets the number of keepalive retries from SCCP to Cisco Unified CME. |
| **Example:** | Router(config-sccp-ccm)# keepalive retries 5 |
| | - `number`—Number of keepalive attempts. Range is 1 to 32. The default is 3. |

| **Step 14** `switchover method [graceful | immediate]` | Sets the switchover method that the SCCP client uses when the communication link between the active Cisco Unified CME system and the SCCP client goes down. |
| **Example:** | Router(config-sccp-ccm)# switchover method immediate |
| | - `graceful`—Switchover happens only after all the active sessions have been terminated gracefully. |
| | - `immediate`—Switches over to any one of the secondary Cisco Unified CME systems immediately. |
### Command or Action | Purpose
--- | ---
**Step 15** 
switchback method (graceful | guard timeout-guard-value | immediate | uptime uptime-timeout-value)  

Example:  
Router(config-sccp-ccm)# switchback method immediate  

Sets the switchover method that the SCCP client uses when the communication link between the active Cisco Unified CME system and the SCCP client goes down.  
- **graceful**—Switchback happens only after all the active sessions have been terminated gracefully.  
- **guard** *timeout-guard-value*—Switchback happens either when the active sessions have been terminated gracefully or when the guard timer expires, whichever happens first. Timeout value is in seconds. Range is from 60 to 172800. Default is 7200.  
- **immediate**—Switches back to the higher order Cisco Unified CME immediately as soon as the timer expires, whether there is an active connection or not.  
- **uptime** *uptime-timeout-value*—Initiates the uptime timer when the higher-order Cisco Unified CME system comes alive. Timeout value is in seconds. Range is from 60 to 172800. Default is 7200.

**Step 16**  
switchback interval *seconds*  

Example:  
Router(config-sccp-ccm)# switchback interval 5  

Sets the amount of time that the DSP farm waits before polling the primary Cisco Unified CME system when the current Cisco Unified CME switchback connection fails.  
- **seconds**—Timer value, in seconds. Range is 1 to 3600. Default is 60.

**Step 17**  
exit  

Example:  
Router(config-sccp-ccm)# exit  

Exits SCCP configuration mode.

**Step 18** 
dspfarm profile *profile-identifier* transcode  

Example:  
Router(config)# dspfarm profile 1 transcode  

Enters DSP farm profile configuration mode and defines a profile for DSP farm services.  
- **profile-identifier**—Number that uniquely identifies a profile. Range is 1 to 65535. There is no default.  
- **transcode**—Enables profile for transcoding.

**Step 19**  
codec *codec-type*  

Example:  
Router(config-dspfarm-profile)# codec g711ulaw  

Specifies the codecs supported by a DSP farm profile.  
- **codec-type**—Specifies the codec preferred.  
  - Use CLI help to locate a list of codecs.

**Step 20**  
maximum sessions *number*  

Example:  
Router(config-dspfarm-profile)# maximum sessions 5  

Specifies the maximum number of sessions that are supported by the profile.  
- **number**—Number of sessions supported by the profile. Range is 0 to X. Default is 0. The X value is determined at run time depending on the number of resources available with the resource provider.
### Configuring Transcoding Support

#### Changing the Number of Transcoding Sessions

Perform this task if you must change the maximum number of DSP farm transcoding sessions.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `no dspfarm`
4. `dspfarm transcoder maximum sessions number`
5. `dspfarm`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router# enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router# configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>
Configuring Cisco Unified CME to Act as the DSP Farm Host

Configuring the Cisco Unified CME router to act as the DSP farm host involves the following:

- Setting the Cisco Unified CME router to receive IP phone messages over the Cisco Unified CME router’s IP address.
- Setting the SCCP server to use a maximum number of DSP farms.
- Setting the Cisco Unified CME router to allow for a maximum number of G.711 and G.729 transcode sessions.
- Tagging and defining DSP farm units for Cisco Unified CME router registry.

To determine the maximum number of transcode sessions that can take place at one time, multiply the maximum number of transcoder sessions you have configured using the `dspfarm transcoder maximum sessions` command by the number of DSP farms in your NM or NM farms. To determine how many DSP farms have been configured, use the `show sdspfarm sessions` and `show sdspfarm units` commands.

The DSP farm units are tagged as 1 through 5 and are defined using the MAC address of the Cisco Unified CME interface. For example, if you have the following configuration:

```plaintext
interface FastEthernet 0/0
 ip address 10.5.49.160 255.255.0.0
 ...  
 sccp local FastEthernet 0/0
 sccp
```

the `show interface FastEthernet 0/0` command will yield a MAC address as shown in the following output:

```plaintext
Router# show interface FastEthernet 0/0
...
 FastEthernet0/0 is up, line protocol is up
 Hardware is AmdFE, address is 000a.8aea.ca80 (bia 000a.8aea.ca80)
```

The MAC address of the Fast Ethernet interface is `000a.8aea.ca80`. 

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 3</strong> no dspfarm</td>
<td>Enables the DSP farm.</td>
</tr>
<tr>
<td>Example: Router(config)# no dspfarm</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> dspfarm transcoder maximum sessions number</td>
<td>Specifies the maximum number of transcoding sessions to be supported by the DSP farm.</td>
</tr>
<tr>
<td>Example: Router(config)# dspfarm transcoder maximum sessions 12</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> dspfarm</td>
<td>Enables the DSP farm.</td>
</tr>
<tr>
<td>Example: Router(config)# dspfarm</td>
<td></td>
</tr>
</tbody>
</table>
You can unregister all active calls’ transcoding streams with the `sdspfarm unregister force` command.

**SUMMARY STEPS**

1. `telephony-service`  
2. `ip source-address ip-address [port port] [any-match | strict-match]`  
3. `sdspfarm units number`  
4. `sdspfarm transcode sessions number`  
5. `sdspfarm tag number device-number`  
6. `exit`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> <code>telephony-service</code></td>
<td>Enters telephony-service configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> `ip source-address ip-address [port port] [any-match</td>
<td>strict-match]`</td>
</tr>
<tr>
<td></td>
<td>• <code>address</code>—The range is 0 through 5. The default is 0.</td>
</tr>
<tr>
<td></td>
<td>• <code>port port</code>—(Optional) TCP/IP port used for Skinny Protocol. The default is 2000.</td>
</tr>
<tr>
<td></td>
<td>• <code>any-match</code>—(Optional) Disables strict IP address checking for registration. This is the default.</td>
</tr>
<tr>
<td></td>
<td>• <code>strict-match</code>—(Optional) Requires strict IP address checking for registration.</td>
</tr>
<tr>
<td><strong>Step 3</strong> <code>sdspfarm units number</code></td>
<td>Specifies the maximum number of DSP farms that are allowed to be registered to the SCCP server.</td>
</tr>
<tr>
<td><strong>Step 4</strong> <code>sdspfarm transcode sessions number</code></td>
<td>Specifies the maximum number of transcoding sessions for G.729 allowed by the Cisco Unified CME router.</td>
</tr>
<tr>
<td></td>
<td>• One transcoding session consists of two transcoding streams between callers using transcoding. Use the maximum number of transcoding sessions and conference calls that you want your router to support at one time.</td>
</tr>
<tr>
<td></td>
<td>• <code>number</code>—The range is 0 through 128. The default is 0.</td>
</tr>
</tbody>
</table>
Transcoding Support

Verifying Transcoding Support

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 5** sdspfarm tag number device-name | Permits a DSP farm unit to be registered to Cisco Unified CME and associates it with an SCCP client interface’s MAC address.  
   - *number*—The tag number. The range is 1 through 5.  
   - *device-name*—The MAC address of the SCCP client interface, with the “mtp” prefix added. |
| Example:                   |                                                                                                                                        |
|   Router(config-telephony)# sdspfarm tag 1 mtp000a8eaca80 |                                                                                                                                        |
| **Step 6** exit            | Exits telephony-service configuration mode.                                                                                           |
| Example:                   |                                                                                                                                        |
|   Router(config-telephony)# exit |                                                                                                                                        |

**Examples**

The following example configures Cisco Unified CME router address 10.100.10.11 port 2000 to act as the farm host using the DSP farm at mtp000a8eaca80 to allow for a maximum of 1 DSP farm and 16 transcode sessions:

```
telephony-service
ip source address 10.100.10.11 port 2000
sdspfarm units 1
sdspfarm transcode sessions 16
sdspfarm tag 1 mtp000a8eaca80
exit
```

**Verifying Transcoding Support**

**Step 1** Use the `show running-config` command to verify the DSP farm commands in the configuration. Refer to the telephony-service portion of the output for commands that set up the Cisco Unified CME router as the DSP farm host.

**Examples**

This section provides the following configuration examples:

- NM-HDV: Example, page 216
- NM-HD and NM-HDV2: Example, page 216
NM-HDV: Example

The following configuration example sets up a DSP farm of 4 DSPs to handle up to 16 sessions (4 sessions per DSP) on a router with an IP address of 10.5.49.160 and a priority of 1 among other servers:

```
voice-card 1
dsp services dspfarm
exit
sccp local FastEthernet 0/0
sccp
sccp ccm 10.5.49.160 priority 1
dspfarm transcoder maximum sessions 16
dspfarm

telephony-service
ip source-address 10.5.49.200 port 2000
sdspfarm units 4
sdspfarm transcode sessions 40
sdspfarm tag 1 mtp000a8eaca80
sdspfarm tag 2 mtp12345672012
```

NM-HD and NM-HDV2: Example

The following example shows a transcoding configuration for a Cisco Unified CME router with either an NM-HD or NM-HDV2. The configuration example sets up six transcoding sessions on a router with one DSP farm, an IP address of 10.5.49.160, and a priority of 1 among servers.

```
voice-card 1
dsp services dspfarm

sccp local FastEthernet 0/1
sccp
sccp ccm 10.5.49.160 identifier 1
sccp ccm group 123
associate ccm 1 priority
associate profile 1 register mtp123456792012
keepalive retries 5
switchover method immediate
switchback method immediate
switchback interval 5

dspfarm profile 1 transcode
codec g711ulaw
codec g711alaw
codec g729ar8
codec g719abr8
maximum sessions 6
associate application sccp

telephony-service
ip source-address 10.5.49.200 port 2000
sdspfarm units 1
sdspfarm transcode sessions 40
sdspfarm tag 1 mtp000a8eaca80
sdspfarm tag 2 mtp12345672012
```
Troubleshooting Transcoding Support

This procedure verifies that a DSP farm is registered and running. You must also ensure that Cisco Unified CME is properly configured to provision transcoding and conferencing resources.

You can clear any of the following features by disabling the DSP farm or SCCP:

- Active calls
- DSPs
- Active (primary) Cisco Unified CME router
- Active connection to a Cisco Unified CME router

If your primary Cisco Unified CME router fails and hands control over to a secondary Cisco Unified CME router, you can switch back to the primary system in either of two ways:

- Graceful switchback: Switches back when active calls on the currently primary system have been terminated.
- Immediate switchback: Switches back immediately.

The following topics are covered in this section:

- Verifying DSP Farm Operation, page 217
- Tuning DSP Farm Performance, page 220

Verifying DSP Farm Operation

To verify that the DSP farm is registered and running, perform the following steps in any order.

**Step 1** Use the `show sccp [statistics | connections]` command to display the SCCP configuration information and current status.

```
Router# show sccp statistics

SCCP Application Service(s) Statistics:

Profile ID:1, Service Type:Transcoding
TCP packets rx 7, tx 7
Unsupported pkts rx 1, Unrecognized pkts rx 0
Register tx 1, successful 1, rejected 0, failed 0
KeepAlive tx 0, successful 0, failed 0
OpenReceiveChannel rx 2, successful 2, failed 0
CloseReceiveChannel rx 0, successful 0, failed 0
StartMediaTransmission rx 2, successful 2, failed 0
StopMediaTransmission rx 0, successful 0, failed 0
Reset rx 0, successful 0, failed 0
MediaStreamingFailure rx 0
Switchover 0, Switchback 0
```
Step 2  Use the `show dspfarm units` command to display the configured and registered DSP farms.

Router# show dspfarm units

mtp-1 Device: MTP003080218a31 TCP socket:[2] REGISTERED
actual_stream: 8 max_stream 8 IP: 10.10.10.3 11470 MTP YOKO keepalive 1
Supported codec: G711Ulaw
G711Alaw
G729a
G729ab

max-mtps: 1, max-streams: 40, alloc-streams: 8, act-streams: 2

Step 3  Use the `show dspfarm sessions` command to display the transcoding streams.

Router# show dspfarm sessions

Stream-ID: 1 mtp: 1 10.10.10.3 18404 Local: 2000 START
usage: Ip-Ip
codec: G711Ulaw64k duration: 20 vad: 0 peer Stream-ID: 2

Stream-ID: 2 mtp: 1 10.10.10.3 17502 Local: 2000 START
usage: Ip-Ip
codec: G729AnnexA duration: 20 vad: 0 peer Stream-ID: 1

Stream-ID: 3 mtp: 1 0.0.0.0 0 Local: 0 IDLE
usage:
codec: G711Ulaw64k duration: 20 vad: 0 peer Stream-ID: 0

Stream-ID: 4 mtp: 1 0.0.0.0 0 Local: 0 IDLE
usage:
codec: G711Ulaw64k duration: 20 vad: 0 peer Stream-ID: 0

Stream-ID: 5 mtp: 1 0.0.0.0 0 Local: 0 IDLE
usage:
codec: G711Ulaw64k duration: 20 vad: 0 peer Stream-ID: 0

Stream-ID: 6 mtp: 1 0.0.0.0 0 Local: 0 IDLE
usage:
codec: G711Ulaw64k duration: 20 vad: 0 peer Stream-ID: 0

Stream-ID: 7 mtp: 1 0.0.0.0 0 Local: 0 IDLE
usage:
codec: G711Ulaw64k duration: 20 vad: 0 peer Stream-ID: 0

Stream-ID: 8 mtp: 1 0.0.0.0 0 Local: 0 IDLE
usage:
codec: G711Ulaw64k duration: 20 vad: 0 peer Stream-ID: 0

Step 4  Use the `show dspfarm sessions summary` command to display a summary view the transcoding streams.

Router# show dspfarm sessions summary

max-mtps: 2, max-streams: 240, alloc-streams: 40, act-streams: 2

<table>
<thead>
<tr>
<th>ID</th>
<th>MTP</th>
<th>State</th>
<th>CallID</th>
<th>confID</th>
<th>Usage</th>
<th>Codec/Duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>IDLE</td>
<td>-1</td>
<td>0</td>
<td></td>
<td>G711Ulaw64k /20ms</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>IDLE</td>
<td>-1</td>
<td>0</td>
<td></td>
<td>G711Ulaw64k /20ms</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>START</td>
<td>-1</td>
<td>3</td>
<td>MoH</td>
<td>G729 /20ms</td>
</tr>
<tr>
<td>4</td>
<td>2</td>
<td>START</td>
<td>-1</td>
<td>3</td>
<td>MoH</td>
<td>G711Ulaw64k /20ms</td>
</tr>
<tr>
<td>5</td>
<td>2</td>
<td>IDLE</td>
<td>-1</td>
<td>0</td>
<td></td>
<td>G711Ulaw64k /20ms</td>
</tr>
<tr>
<td>6</td>
<td>2</td>
<td>IDLE</td>
<td>-1</td>
<td>0</td>
<td></td>
<td>G711Ulaw64k /20ms</td>
</tr>
<tr>
<td>7</td>
<td>2</td>
<td>IDLE</td>
<td>-1</td>
<td>0</td>
<td></td>
<td>G711Ulaw64k /20ms</td>
</tr>
<tr>
<td>8</td>
<td>2</td>
<td>IDLE</td>
<td>-1</td>
<td>0</td>
<td></td>
<td>G711Ulaw64k /20ms</td>
</tr>
</tbody>
</table>
Step 5 Use the show dspfarm sessions active command to display the transcoding streams for all active sessions.

Router# show dspfarm sessions active
Stream-ID:1 mtp:1 10.10.10.3  18404  Local:2000 START
  usage:Ip-Ip
  codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:2

Stream-ID:2 mtp:1 10.10.10.3  17502  Local:2000 START
  usage:Ip-Ip
  codec:G729AnnexA  duration:20 vad:0 peer Stream-ID:1

Step 6 Use the show sccp connections details command to display the SCCP connections details such as call-leg details.

Router# show sccp connections details
bridge-info(bid, cid) - Normal bridge information(Bridge id, Calleg id)
mmbbridge-info(bid, cid) - Mixed mode bridge information(Bridge id, Calleg id)

<table>
<thead>
<tr>
<th>sess_id</th>
<th>conn_id</th>
<th>call-id</th>
<th>codec</th>
<th>pkt-period</th>
<th>type</th>
<th>bridge-info(bid, cid)</th>
<th>mmbbridge-info(bid, cid)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>-</td>
<td>14</td>
<td>N/A</td>
<td>N/A</td>
<td>transmsp</td>
<td>All RTPSPI Callegs</td>
<td>N/A</td>
</tr>
<tr>
<td>1</td>
<td>2</td>
<td>15</td>
<td>g729a</td>
<td>20</td>
<td>rtpspi</td>
<td>(4,14)</td>
<td>N/A</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>13</td>
<td>g711u</td>
<td>20</td>
<td>rtpspi</td>
<td>(3,14)</td>
<td>N/A</td>
</tr>
</tbody>
</table>

Total number of active session(s) 1, connection(s) 2, and callegs 3

Step 7 Use the debug sccp {all|errors|events|packets|parser} command to set debugging levels for SCCP and its applications.
Step 8 Use the `debug dspfarm {all | errors | events | packets}` command to set debugging levels for DSP-farm service.

Step 9 Use the `debug ephone mtp` command to enable Message Transfer Part (MTP) debugging. Use this debug command with the `debug ephone mtp, debug ephone register, debug ephone state, and debug ephone pak` commands.

---

**Tuning DSP Farm Performance**

This task tunes DSP farm performance.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `sccp ip precedence value`
4. `dspfarm rtp timeout seconds`
5. `dspfarm connection interval seconds`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td>Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> <code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> <code>sccp ip precedence value</code></td>
<td>(Optional) Sets the IP precedence value.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# sccp ip precedence 5</td>
<td>Doing so allows you to increase the priority of voice packets over connections controlled by SCCP.</td>
</tr>
<tr>
<td><strong>Step 4</strong> <code>dspfarm rtp timeout seconds</code></td>
<td>(Optional) Configures the Real-Time Transport Protocol (RTP) timeout interval for when the error condition “RTP port unreachable” occurs.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# dspfarm rtp timeout 60</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> <code>dspfarm connection interval seconds</code></td>
<td>(Optional) Specifies how long to monitor RTP inactivity before deleting an RTP stream.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# dspfarm connection interval 60</td>
<td></td>
</tr>
</tbody>
</table>
Feature History for Transcoding Support

<table>
<thead>
<tr>
<th>Cisco Unified CME Version</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.2</td>
<td>Transcoding between G.711 and G.729 was introduced.</td>
</tr>
</tbody>
</table>

Related Features

Teleworker Remote Phones
Transcoding has benefits and disadvantages for teleworker remote phones. See the discussion in the “Teleworker Remote Phones” section on page 143.

Music on Hold
Music on hold can require transcoding resources. See the “Music on Hold” section on page 333.
transfer and forwarding support

This module describes Cisco Unified CallManager Express (Cisco Unified CME) transfer and forwarding support for interworking with various network requirements. It contains the following sections:

- Transfer and Forwarding Support Overview, page 223
- Configuring Transfer and Forwarding Support, page 238
- Verifying Transfer and Forwarding Support, page 256
- Examples, page 256
- Troubleshooting Transfer and Forwarding Support, page 260
- Feature History for Transfer and Forwarding Support, page 261
- Related Features, page 262

Note Prior to version 4.0, the name of this product was Cisco CallManager Express (Cisco CME). Prior to version 3.0, the name was Cisco IOS Telephony Services (Cisco ITS).


transfer and forwarding support overview

Note For a summary of the functionality introduced in different releases, see the “Feature History for Transfer and Forwarding Support” section on page 261.
Note
Cisco CallManager Express 3.2 (Cisco CME 3.2) and later versions provide full call-transfer and call-forwarding interoperability with call processing systems on the network that support H.450.2, H.450.3, and H.450.12 standards. For call processing systems that do not support H.450 standards, Cisco CME 3.2 and later versions provide VoIP-to-VoIP hairpin call routing without requiring the use of the special Tool Command Language (Tcl) script that was needed in earlier releases of Cisco CME.

This section covers the following topics:

- Background, page 224
- Strategies for Call Transfer and Call Forwarding, page 225
- Typical Network Scenarios for Call Transfer and Call Forwarding, page 233

Background

In a mixed network that involves two or more types of call agents or managers, there can be communication protocol discrepancies and dependencies, and therefore the opportunity for interoperability errors. These discrepancies show up most often when a call is being transferred or forwarded. The following recent Cisco CME releases have introduced features to address these discrepancies and enable transparent transferring and forwarding of calls across VoIP networks.

Cisco IOS Telephony Services V2.1 (Cisco ITS V2.1), Cisco IOS Release 12.2(15)T
Cisco ITS V2.1 was the predecessor to Cisco CME 3.0. Prior to Cisco ITS V2.1, call transfer was performed using a Cisco proprietary method. Cisco ITS V2.1 introduced support for call transfer using the ITU-T H.450.2 standard, which was configured using the `transfer-system` command and a Tcl application script. Similarly, call forwarding using the H.450.3 standard was supported in Cisco ITS V2.1 and was configured using the `call forward pattern` command and the same Tcl script. To configure Cisco ITS V2.1 systems for call transfer and call forwarding, refer to the Cisco IOS Telephony Services Version 2.1 guide.

Cisco CME 3.0, Cisco IOS Release 12.2(15)ZJ
Cisco CME 3.0 added support for IP phones to initiate call transfer using the H.450.2 protocol and call forwarding using the H.450.3 protocol by using the default session application. The built-in H.450.2 and H.450.3 support that is provided by the default session application applied to call transfers and forwards initiated by IP phones, regardless of public switched telephone network (PSTN) interface type. In order to use this feature, however, all endpoints in the VoIP network were required to support the H.450.2 and H.450.3 standards. There was no fallback for other types of endpoints and no way to detect which endpoints supported the standards. To configure Cisco CME 3.0 systems for call transfer and call forwarding, refer to the Cisco CallManager Express 3.0 System Administrator Guide.

Cisco CME 3.0, Cisco IOS Releases 12.2(15)ZJ3 and 12.3(4)T
To handle calls to endpoints that did not recognize the H.450 standards, Cisco CME 3.0 in Cisco IOS Releases 12.2(15)ZJ3 and 12.3(4)T introduced a new Tcl script that enabled hairpin VoIP-to-VoIP call routing for transfers and forwards on the Cisco CME router. Hairpin call routing uses the Cisco CME router to reoriginate a terminated call and route it as appropriate to complete a transfer or forward generated by a phone or other application attached to the router. There was still no way to automatically identify which endpoints supported H.450 standards, and hairpin call routing has the disadvantage of using two calls’ worth of bandwidth for the duration of the transferred or forwarded call. To configure Cisco CME 3.0 systems for call transfer and call forwarding, refer to the Cisco CallManager Express 3.0 System Administrator Guide.
Cisco CME 3.1, Cisco IOS Release 12.3(7)T

Cisco CME 3.1 introduces support for H.450.12 supplementary services, which provide dynamic detection of H.450.2 and H.450.3 capabilities on a call-by-call basis. Calls that can be transferred or forwarded to an H.450 endpoint are handled using H.450 standard protocols, while other calls are handled by a fallback method. Note that although Cisco CME 3.0 and Cisco ITS V2.1 both support H450.2 and H.450.3 standards, they do not support H.450.12. Therefore, Cisco CME 3.0 and Cisco ITS V2.1 systems cannot automatically detect whether endpoints are capable of using the H.450.2 and H.450.3 standards.

Cisco CME 3.1 supports two fallback methods for calls to endpoints that do not support H.450 standards: hairpin call routing and H.450 tandem gateways. Hairpin call routing was first supported in Cisco CME 3.0 using a Tcl script. In Cisco CME 3.1, hairpin call routing is enabled using Cisco IOS command-line interface (CLI) commands rather than a Tcl script, thus simplifying its implementation.

H.450 tandem gateways address the limitations of hairpin call routing. An H.450 tandem gateway is an additional voice gateway that serves as a “front-end” for a call processor that does not support the H.450 standards, such as Cisco Unified CallManager, Cisco BTS Softswitch (Cisco BTS), or Cisco PSTN Gateway (Cisco PGW). Transferred and forwarded calls that are intended for non-H.450 endpoints are terminated instead on the H.450 tandem gateway and reoriginated there for delivery to the non-H.450 endpoints. The H.450 tandem gateway can also serve as a PSTN gateway. To configure Cisco CME 3.0 systems for call transfer and call forwarding, refer to the Cisco CallManager Express 3.1 System Administrator Guide.

Cisco CME 3.2, Cisco IOS Release 12.3(11)T

Transcoding between G.711 and G.729 is supported when one leg of a Voice over IP (VoIP)-to-VoIP hairpin call uses G.711 and the other leg uses G.729. For information about transcoding, refer to the “Transcoding Support” section on page 199 chapter of this guide.

H.323-to-SIP connections are allowed only for Cisco Unified CME systems running Cisco Unity Express. For more information, refer to Integrating Cisco CallManager Express with Cisco Unity Express.

Strategies for Call Transfer and Call Forwarding

As mentioned in the “Background” section on page 224, the risk of discrepancies among dissimilar call processing systems exists in the handling of transferred and forwarded calls. This section describes the following strategies for handling transferred and forwarded calls:

- H.450.2 and H.450.3 Support, page 225
- H.450.12 Support, page 228
- Hairpin Call Routing, page 229
- H.450 Tandem Gateways, page 231

H.450.2 and H.450.3 Support

Cisco CME 3.1 and later continues the support for the H.450.2 call-transfer standards and the H.450.3 call-forwarding standards that was introduced in Cisco ITS V2.1. Use of the H.450.2 and H.450.3 standards is the best way to handle call transfer and forwarding in a VoIP network and provides the following benefits:

- The final call path from the transferred party to the transfer destination is optimal, with no hairpinned routes or excessive use of resources.
- Call parameters (for example, codec) can be different for the different call legs.
- This solution is scalable.
- There is no limit to the number of times a call can be transferred.

Considerations for using the H.450.2 and H.450.3 standards include the following:

- Cisco IOS Release 12.2(15)T or a later release is required on all voice gateways in the network.
- Support of H.450.2 and H.450.3 is required on all voice gateways in the network. H.450.2 and H.450.3 are used even when the transfer-to or forward-to target is on the same Cisco CME system as the transferring party or the forwarding party, so the transferred party must also support H.450.2 and the forwarded party must also support H.450.3. The exception to this rule is calls that can be reoriginated through hairpin call routing or through the use of an H.450 tandem gateway.
- H.450 standards are not supported by Cisco Unified CallManager, Cisco BTS, or Cisco PGW, although hairpin call routing or an H.450 tandem gateway can be set up to handle calls to and from those types of systems.

The following series of figures depicts a call being transferred using H.450.2 standards. Figure 20 on page 226 shows that a call has been made from A to B. Figure 21 on page 226 shows B consulting with C and putting A on hold. Figure 22 on page 226 shows that B has connected A and C, and Figure 23 on page 227 shows A and C directly connected, with B no longer involved in the call.

**Figure 20**  
Call Transfer Using H.450.2: A Calls B

**Figure 21**  
Call Transfer Using H.450.2: B Consults with C
Use H.450 standards when a network meets the following conditions:

- The router that you are configuring uses Cisco CME 3.0 and later, or Cisco ITS V2.1.
- For Cisco CME 3.0 or Cisco ITS V2.1 systems, all endpoints in the network must support H.450.2 and H.450.3 standards. For Cisco CME 3.1 systems, if some of the endpoints do not support H.450 standards (for example, Cisco Unified CallManager, Cisco BTS, or Cisco PGW), you can use hairpin call routing or an H.450 tandem gateway to handle transfers and forwards with those endpoints. Also, either you must explicitly disable H.450.2 and H.450.3 on the dial peers that handle those calls or you must enable H.450.12 capability to automatically detect the calls that support H.450.2 and H.450.3 and those calls that do not.

Support for the H.450.2 standard and the H.450.3 standard is enabled by default and can be disabled globally or for individual dial peers using the supplementary-service h450.2 and supplementary-service h450.3 commands. Settings made for individual dial peers override the global setting. For configuration information, see the “Enabling or Disabling H.450.2 and H.450.3 Capabilities” section on page 240.
H.450.12 Support

Cisco CME 3.1 and later versions support the H.450.12 call capabilities standard, which provides a means to advertise and dynamically discover H.450.2 and H.450.3 capabilities in voice gateway endpoints. Once discovered, the calls associated with non-H.450 endpoints can be directed to use non-H.450 methods for transfer and forwarding, such as hairpin call routing or H.450 tandem gateway.

You can have either of the following situations in your network:

- All gateway endpoints support H.450.2 and H.450.3 standards. In this situation, no special configuration is required because support for H.450.2 and H.450.3 standards is enabled on the Cisco CME 3.1 or later router by default. H.450.12 capability is disabled by default, but it is not required because all calls can use H.450.2 and H.450.3 standards.

- Some gateway endpoints support H.450.2 and H.450.3 standards, and other gateway endpoints do not. In this situation, you need to specify how non-H.450 calls are to be handled by choosing one of the following options:
  - Use the H.450.12 capability in Cisco CME 3.1 and later to dynamically determine, on a call-by-call basis, whether each call has H.450.2 and H.450.3 support. To use this option, you must explicitly enable H.450.12 capability in the router configuration because it is disabled by default. If H.450.12 is enabled and a call is determined to have H.450 support, the call is transferred using H.450.2 standards or forwarded using H.450.3 standards. If the call does not have H.450 support, it can be handled by a VoIP-to-VoIP connection that you set up using dial peers and the **allow connections** command. The VoIP-to-VoIP connection can be used for hairpin call routing or routing to an H.450 tandem gateway. The following commands enable H.450.12 capability and enable H.323 VoIP-to-VoIP connections:

    Router(config)# voice service voip
    Router(config-voice-service)# supplementary-service h450.12
    Router(config-voice-service)# allow connections h323 to h323

    Note that you can enable the **supplementary-service h450.12** command in dial-peer configuration mode to target specific dial peers if you do not want to enable the capability globally.

    - Your second choice for handling non-H.450 calls is to explicitly disable H.450.2 and H.450.3 capability on a global basis or by individual dial peer, which forces all calls to be handled by the VoIP-to-VoIP connection that you have set up using dial peers and the **allow connections** command. This connection can be used for hairpin call routing or routing to an H.450 tandem gateway. The following commands globally disable H.450.2 and H.450.3 standards and enable H.323 VoIP-to-VoIP connections:

        Router(config)# voice service voip
        Router(config-voice-service)# no supplementary-service h450.2
        Router(config-voice-service)# no supplementary-service h450.3
        Router(config-voice-service)# allow connections h323 to h323

Support for the H.450.12 standard is disabled by default. It can be enabled or disabled globally and can be enabled for individual dial peers if it is disabled globally. Settings made for individual dial peers override the global setting. For configuration information, see the "Enabling or Disabling H.450.12 Capabilities" section on page 245.
Hairpin Call Routing

Hairpin call routing uses the VoIP-to-VoIP connection mechanisms that were introduced in Cisco CME 3.1 to transfer and forward calls that cannot use H.450 standards. When a call that originally terminated on a voice gateway is transferred or forwarded by a phone or other application attached to the gateway, the gateway reoriginates the call and routes the call as appropriate, making a VoIP-to-VoIP, or hairpin, connection. This approach avoids any protocol dependency on the far-end transferred-party endpoint or transfer-destination endpoint. Hairpin routing of transferred and forwarded calls also causes the generation of separate billing records for each call leg, so that the transferred or forwarded call leg is typically billed to the user who initiates the transfer or forward.

For Cisco CME 3.2 and later versions, transcoding between G.711 and G.729 is supported when one leg of a VoIP-to-VoIP hairpin call uses G.711 and the other leg uses G.729. For information about transcoding, refer to the “Transcoding Support” section on page 199 chapter of this guide.

Hairpin call routing provides the following benefits:

- Call transfer and forwarding is provided to non-H.450 endpoints, such as Cisco Unified CallManager, Cisco BTS, or Cisco PGW.
- The network can also contain Cisco CME 3.0 or Cisco ITS 2.1 systems.

Hairpin call routing has the following disadvantages:

- End-to-end signaling and media delay are increased significantly.
- A single hairpinned call uses as much WAN bandwidth as two directly connected calls.

VoIP-to-VoIP hairpin connections can be made using dial peers if the allow-connections h323 to h323 command is enabled and at least one of the following is true:

- H.450.12 is used to detect calls on which H.450.2 or H.450.3 is not supported by the remote system.
- H.450.2 or H.450.3 is explicitly disabled.
- Cisco CME automatically detects that the remote system is a Cisco Unified CallManager.

Figure 24 on page 229 shows a call that is made from A to B. Figure 25 on page 230 shows that B has forwarded all calls to C. Figure 26 on page 230 shows that A and C are connected by an H.323 hairpin.
Use hairpin call routing when a network meets the following three conditions:

- The router that you are configuring uses Cisco CME 3.1 or a later release.
- Some or all calls require VoIP-to-VoIP routing because they cannot use H.450 standards, which can happen for any of the following reasons:
  - H.450 capabilities have been explicitly disabled on the router.
  - H.450 capabilities do not exist in the network.
  - H.450 capabilities are supported on some endpoints and not supported on other endpoints, including those handled by Cisco Unified CallManager, Cisco BTS, and Cisco PGW. When some endpoints support H.450 and others do not, you must enable H.450.12 capabilities on the router to detect which endpoints are H.450-capable or designate some dial peers as H.450-capable. For more information about enabling H.450.12 capabilities, see the “Enabling or Disabling H.450.12 Capabilities” section on page 245.
- No voice gateway is available to act as an H.450 tandem gateway.

Support for VoIP-to-VoIP connections is disabled by default and can be enabled globally using the allow connections h323 to h323 command. For configuration information, see the “Enabling H.323-to-H.323 Connection Capabilities” section on page 248.
Restrictions

Only one codec type is supported in the VoIP network at a time, and there are only two codec choices: G.711 (A-law or mu-law) or G.729.

H.450 Tandem Gateways

An H.450 tandem voice gateway terminates and reorignates calls to be transferred and forwarded to endpoints that do not support H.450 standards, in a manner similar to hairpin call routing but without the double WAN link traversal created by hairpin connections. An H.450 tandem gateway is a separate router that provides a proxy, or “front-end,” for a system that does not support H.450 standards, such as a Cisco Unified CallManager system. Figure 27 on page 232 shows a tandem voice gateway that has been placed between the central hub of the network of a CPE-based Cisco CME 3.1 or later network and a Cisco Unified CallManager network. This topology would work equally well with a Cisco BTS or Cisco PGW in place of the Cisco Unified CallManager. An H.450 tandem gateway can also work as a PSTN gateway for remote Cisco Unified CME systems and for Cisco Unified CallManager (or other non-H.450 system). Use different inbound dial peers to separate Cisco Unified CallManager-to-PSTN G.711 calls from tandem gateway-to-Cisco Unified CME G.729 calls.

An H.450 tandem gateway is configured with a dial peer that points to the Cisco Unified CallManager or other system for which the H.450 tandem gateway is serving as a front end. The H.450 tandem voice gateway is also configured with dial peers that point to all the Cisco Unified CME systems in the private H.450 network. In this way, Cisco Unified CME and the Cisco Unified CallManager are not directly linked to each other, but are instead both linked to an H.450 tandem gateway that provides H.450 services to the non-H.450 platform.

Note

An H.450 tandem gateway that is used in a network to support non-H.450-capable call processing systems requires the Integrated Voice and Video Services feature license. This feature license, which was introduced in March 2004, includes functionality for H.323 gatekeeper, IP-to-IP Gateway, and H.450 tandem gateway. With Cisco IOS Release 12.3(7)T, an H.323 gatekeeper feature license is required with a JSX IOS image on the selected router. Please consult your Cisco Unified CME SE regarding the required feature license. With Cisco IOS Release 12.3(7)T, you cannot use Cisco Unified CME and H.450 tandem gateway functionality on the same router.

VoIP-to-VoIP connections can be made for an H.450 tandem gateway if the **allow-connections h323 to h323** command is enabled and one or more of the following is true:

- H.450.12 is used to dynamically detect calls on which H.450.2 or H.450.3 is not supported by the remote VoIP system.
- H.450.2 or H.450.3 is explicitly disabled.
- Cisco CME 3.1 or later automatically detects that the remote system is a Cisco Unified CallManager.

For Cisco CME 3.1 and earlier, the only type of VoIP-to-VoIP connection supported by Cisco CME is H.323-to-H.323. For Cisco CME 3.2 and later versions, H.323-to-SIP connections are allowed only for Cisco CME systems running Cisco Unity Express. For more information, see *Integrating Cisco CallManager Express and Cisco Unity Express*. 
In the network topology in Figure 27 on page 232, the following events occur (refer to the event numbers on the illustration):

1. A call is generated from extension 4002 on phone 2, which is connected to a Cisco Unified CallManager. The H.450 tandem gateway receives the H.323 call and, acting as the H.323 endpoint, the H.450 tandem gateway handles the call connection to a Cisco Unified IP phone in a CPE-based Cisco CME 3.1 or later network.

2. The call is received by extension 1001 on phone 3, which is connected to Cisco Unified CME 1. Extension 1001 performs a consultation transfer to extension 2001 on phone 5, which is connected to Cisco Unified CME 2.

3. When extension 1001 transfers the call, the H.450 tandem gateway receives an H.450.2 message from extension 1001.

4. The H.450 tandem gateway terminates the call leg from extension 1001 and reoriginates a call leg to extension 2001, which is connected to Cisco Unified CME 2.

5. Extension 4002 is connected with extension 2001.
Use this method when a network meets the following conditions:

- The router that you are configuring uses Cisco CME 3.1 or a later version.
- Some endpoints in the network are not H.450-capable, including those handled by Cisco Unified CallManager, Cisco BTS, and Cisco PGW.

Support for VoIP-to-VoIP connections is disabled by default and can be enabled globally using the `allow connections h323 to h323` command. For more information, see the “Enabling H.323-to-H.323 Connection Capabilities” section on page 248.

Use dial peers to set up an H.450 tandem gateway. See the “Setting Up Dial Peers” section on page 256.

**Restrictions**

- Cisco Unified CallManager must use a media termination point (MTP), intercluster trunk (ICT) mode, and slow start.
- Codecs on all the VoIP dial peers of the H.450 tandem gateway must be the same.
- Only one codec type is supported in the VoIP network at a time, and there are only two codec choices: G.711 (A-law or mu-law) or G.729.
- Transcoding is not supported.
- Codec renegotiation is not supported. For example, if an H.323 call that uses a G.729 codec is received by a Cisco Unified CME system and is forwarded to a voice-mail system that requires a G.711 codec, the codec cannot be renegotiated from G.729 to G.711.

**Typical Network Scenarios for Call Transfer and Call Forwarding**

This section provides descriptions of the specific mixed-network scenarios that you might encounter when configuring a router running Cisco CME 3.1 or a later version. Each description points to the configuration instructions necessary to ensure call transfer and forwarding capabilities throughout the network. The following descriptions are provided:

- Cisco CME 3.1 or Later and Cisco IOS Gateways, page 233
- Cisco CME 3.1 or Later, Cisco CME 3.0 or Cisco ITS V2.1, and Cisco IOS Gateways, page 234
- Cisco CME 3.1 or Later, Non-H.450 Gateways, and Cisco IOS Gateways, page 235
- Cisco CME 3.1 or Later, Cisco CME 3.0 or Cisco ITS V2.1, Non-H.450 Gateways, and Cisco IOS Gateways, page 235
- Cisco CME 3.1 or Later, Cisco Unified CallManager, and Cisco IOS Gateways, page 236
- Cisco CME 3.1 or Later, Cisco CME 3.0 or Cisco ITS V2.1, Cisco Unified CallManager, and Cisco IOS Gateways, page 237

**Cisco CME 3.1 or Later and Cisco IOS Gateways**

A network with Cisco CME 3.1 and Cisco IOS gateways can contain the following types of systems:

- Cisco CME 3.1 or later
- Cisco IOS gateways

In this scenario, all systems that might participate in calls that involve call transfer and call forwarding are capable of supporting the H.450.2, H.450.3, and H.450.12 standards. This is the simplest environment for operating the Cisco CME 3.1 or later features.
Configuration for this type of network consists of the following general steps:

1. Set up call-transfer and call-forwarding parameters for transfers and forwards that are initiated on this router (H.450.2 and H.450.3 capabilities for transferred parties, transfer destinations, forwarded parties, and forwarding destinations are enabled by default). See the “Enabling or Disabling H.450.2 and H.450.3 Capabilities” section on page 240.

2. Enable H.450.12 globally to detect any calls on which H.450.2 and H.450.3 standards are not supported. Although this step is optional, it is recommended. See the “Enabling or Disabling H.450.12 Capabilities” section on page 245.

3. Optionally set up VoIP-to-VoIP connections (hairpin call routing or H.450 tandem gateway) to route calls that do not support H.450.2 or H.450.3 standards. See the “Enabling H.323-to-H.323 Connection Capabilities” section on page 248.

4. Set up dial peers to manage call legs within the network. See the “Setting Up Dial Peers” section on page 256.

Cisco CME 3.1 or Later, Cisco CME 3.0 or Cisco ITS V2.1, and Cisco IOS Gateways

A network with Cisco CME 3.1 or later, Cisco CME 3.0 or Cisco ITS V2.1, and Cisco IOS gateways can contain a combination of the following types of systems:

- Cisco CME 3.1 or later
- Cisco CME 3.0
- Cisco ITS V2.1
- Cisco IOS gateways

You might have this type of network while you are in the process of upgrading a Cisco CME 3.0 network to Cisco CME 3.1 or later. Both Cisco CME 3.1 or later and Cisco CME 3.0 routers assume that H.450.2 and H.450.3 standards are to be used for all calls. Note that Cisco CME 3.0 and Cisco ITS 2.1 do not support the H.450.12 standard.

Configuration for this type of network consists of the following general steps:

1. Set up call-transfer and call-forwarding parameters for transfers and forwards that are initiated on this router (H.450.2 and H.450.3 capabilities for transferred parties, transfer destinations, forwarded parties, and forwarding destinations are enabled by default). See the “Enabling or Disabling H.450.2 and H.450.3 Capabilities” section on page 240.

2. Enable H.450.12 in advertise-only mode on Cisco CME 3.1 or later systems. As each Cisco CME 3.0 system is upgraded to Cisco CME 3.1 or later, enable H.450.12 in advertise-only mode. Note that no checking for H.450.2 or H.450.3 support is done in advertise-only mode. When all Cisco CME 3.0 systems in the network have been upgraded to Cisco CME 3.1 or later, remove the advertise-only restriction. See the “Enabling or Disabling H.450.12 Capabilities” section on page 245.

3. Optionally set up VoIP-to-VoIP connections (hairpin call routing or H.450 tandem gateway) to route calls that cannot use H.450.2 or H.450.3 standards. See the “Enabling H.323-to-H.323 Connection Capabilities” section on page 248.

4. Set up dial peers to manage call legs within the network. See the “Setting Up Dial Peers” section on page 256.
Cisco CME 3.1 or Later, Non-H.450 Gateways, and Cisco IOS Gateways

A network with Cisco CME 3.1 or later, non-H.450 gateways, and Cisco IOS gateways can contain a combination of the following types of systems:

- Cisco CME 3.1 or later
- Gateways that do not support H.450.2 and H.450.3 standards, such as Cisco Unified CallManager, Cisco BTS, or Cisco PGW systems
- Cisco IOS gateways

In this type of network, the H.450.2 and H.450.3 services are provided only to calling endpoints that use H.450.12 to explicitly indicate that they are capable of H.450.2 and H.450.3 operations. Because the current releases of Cisco BTS and Cisco PGW do not support the H.450.12 standard, calls to and from these systems that involve call transfer or forwarding are handled with H.323-to-H.323 hairpin call routing.

Configuration for this type of network consists of the following general steps:

1. Set up call-transfer and call-forwarding parameters for transfers and forwards that are initiated on this router (H.450.2 and H.450.3 capabilities for transferred parties, transfer destinations, forwarded parties, and forwarding destinations are enabled by default). Optionally disable H.450.2 and H.450.3 capabilities on dial peers that point to non-H.450-capable systems such as Cisco Unified CallManager, Cisco BTS, or Cisco PGW. See the “Enabling or Disabling H.450.2 and H.450.3 Capabilities” section on page 240.

2. Enable H.450.12 to detect any calls on which H.450.2 and H.450.3 standards are not supported, either globally or for specific dial peers. See the “Enabling or Disabling H.450.12 Capabilities” section on page 245.

3. Set up VoIP-to-VoIP connections (hairpin call routing or H.450 tandem gateway) to route calls that do not support H.450.2 or H.450.3 standards. See the “Enabling H.323-to-H.323 Connection Capabilities” section on page 248.

4. Set up dial peers to manage call legs within the network. See the “Setting Up Dial Peers” section on page 256.

Note

If your network contains a Cisco Unified CallManager, also see the instructions in the “Enabling Interworking with Cisco Unified CallManager” section on page 249.

Cisco CME 3.1 or Later, Cisco CME 3.0 or Cisco ITS V2.1, Non-H.450 Gateways, and Cisco IOS Gateways

A network with Cisco CME 3.1 or later, Cisco CME 3.0 or Cisco ITS V2.1, non-H.450 gateways, and Cisco IOS gateways can contain a combination of the following types of systems:

- Cisco CME 3.1 or later
- Cisco CME 3.0
- Cisco ITS V2.1
- Gateways that do not support H.450.2 and H.450.3 standards, such as Cisco Unified CallManager, Cisco BTS, or Cisco PGW systems
- Cisco IOS gateways
This type of network contains a mix of Cisco Unified CME versions and at least one non-H.450 gateway. Cisco CME 3.0 and Cisco ITS V2.1 systems do not have H.450.12 capabilities. The simplest configuration approach for this type of network is to globally disable all H.450.2 and H.450.3 services and force H.323-to-H.323 hairpin call routing for all transferred and forwarded calls. In this case, you would enable H.450.12 detection capabilities globally. Alternatively, you could select to enable H.450.12 capability for specific dial peers. In this case, you would not configure H.450.12 capability globally; you would leave it in its default disabled state.

Configuration for this type of network consists of the following general steps:

1. Set up call-transfer and call-forwarding parameters for transfers and forwards that are initiated on this router (H.450.2 and H.450.3 capabilities for transferred parties, transfer destinations, forwarded parties, and forwarding destinations are enabled by default). See the “Enabling or Disabling H.450.2 and H.450.3 Capabilities” section on page 240.

2. Enable H.450.12 to detect any calls on which H.450.2 and H.450.3 standards are not supported, either globally or on specific dial peers. See the “Enabling or Disabling H.450.12 Capabilities” section on page 245.

3. Set up VoIP-to-VoIP connections (hairpin call routing or H.450 tandem gateway) to route all transferred and forwarded calls. See the “Enabling H.323-to-H.323 Connection Capabilities” section on page 248.

4. Set up dial peers to manage call legs within the network. See the “Setting Up Dial Peers” section on page 256.

If your network contains a Cisco Unified CallManager, also see the instructions in the “Enabling Interworking with Cisco Unified CallManager” section on page 249.

Cisco CME 3.1 or Later, Cisco Unified CallManager, and Cisco IOS Gateways

A network with Cisco CME 3.1 or later, Cisco Unified CallManager, and Cisco IOS gateways can contain a combination of the following types of systems:

- Cisco CME 3.1 or later
- Cisco Unified CallManager
- Cisco IOS gateways

This type of network contains only Cisco CME 3.1 or later systems and Cisco Unified CallManager systems. The Cisco CME 3.1 or later release supports automatic detection of calls to and from Cisco Unified CallManager using proprietary signaling elements that are included with the standard H.323 message exchanges. The Cisco CME 3.1 or later system uses these detection results to determine the H.450.2 and H.450.3 capabilities of calls rather than using H.450.12 supplementary services capabilities exchange, which Cisco Unified CallManager does not support. If a call is detected to be coming from or going to a Cisco Unified CallManager endpoint, the call is treated as a non-H.450 call. All other calls in this type of network are treated as though they support H.450 standards. Therefore, this type of network should contain only Cisco CME 3.1 or later and Cisco Unified CallManager call-processing systems.

Configuration for this type of network consists of the following general steps:

1. Set up call-transfer and call-forwarding parameters for transfers and forwards that are initiated on this router (H.450.2 and H.450.3 capabilities for transferred parties, transfer destinations, forwarded parties, and forwarding destinations are enabled by default). See the “Enabling or Disabling H.450.2 and H.450.3 Capabilities” section on page 240.
2. Enable H.450.12 to detect any calls on which H.450.2 and H.450.3 standards are not supported, either globally or on specific dial peers. See the “Enabling or Disabling H.450.12 Capabilities” section on page 245.

3. Set up VoIP-to-VoIP connections (hairpin call routing or H.450 tandem gateway) to route all transferred and forwarded calls that are detected as being to or from Cisco Unified CallManager. See the “Enabling H.323-to-H.323 Connection Capabilities” section on page 248.

4. Set up specific parameters for Cisco Unified CallManager. See the instructions in the “Enabling Interworking with Cisco Unified CallManager” section on page 249.

5. Set up dial peers to manage call legs within the network. See the “Setting Up Dial Peers” section on page 256.

**Cisco CME 3.1 or Later, Cisco CME 3.0 or Cisco ITS V2.1, Cisco Unified CallManager, and Cisco IOS Gateways**

A network with Cisco CME 3.1 or later, Cisco CME 3.0 or Cisco ITS V2.1, Cisco Unified CallManager, and Cisco IOS gateways can contain a combination of the following types of systems:

- Cisco CME 3.1 or later
- Cisco CME 3.0
- Cisco ITS V2.1
- Cisco Unified CallManager
- Cisco IOS gateways

Calls between the Cisco Unified CallManager and the older Cisco CME 3.0 or Cisco ITS V2.1 networks need special consideration. Because Cisco CME 3.0 and Cisco ITS V2.1 systems do not support automatic Cisco Unified CallManager detection and also do not natively support H.323-to-H.323 call routing, alternative arrangements are required for these systems.

To configure call transfer and forwarding on the Cisco CME 3.0 router, you can select from the following three options:

- Use a Tcl script to handle call transfer and forwarding by invoking Tcl-script-based H.323-to-H.323 hairpin call routing (app-h450-transfer.2.0.0.9.tcl or a later version). Enable this script on all VoIP dial peers and also under telephony-service mode, and set the local-hairpin script parameter to 1. Refer to the configuration instructions in the “Configuring Call Transfer” chapter of the *Cisco CallManager Express 3.0 System Administrator Guide*.

- Use a loopback-dn mechanism. Refer to the instructions in the “Loopback Call Routing” appendix of the *Cisco CallManager Express 3.0 System Administrator Guide*.

- Configure a loopback call path using router physical voice ports.

All three options force use of H.323-to-H.323 hairpin call routing for all calls irrespective of whether the call is from a Cisco Unified CallManager or other H.323 endpoint (including Cisco CME 3.1 or later).

In addition to the special considerations above, configuration of the Cisco CME 3.1 or later router for this type of network consists of the following general steps:

1. Set up call-transfer and call-forwarding parameters for transfers and forwards that are initiated on this router (H.450.2 and H.450.3 capabilities for transferred parties, transfer destinations, forwarded parties, and forwarding destinations are enabled by default). See the “Enabling or Disabling H.450.2 and H.450.3 Capabilities” section on page 240.
2. Leave H.450.12 capability in its default disabled state. For more information, see the “Enabling or Disabling H.450.12 Capabilities” section on page 245.

3. Set up VoIP-to-VoIP connections (hairpin call routing or H.450 tandem gateway) to route all transferred and forwarded calls that are detected as being to or from Cisco Unified CallManager. See the “Enabling H.323-to-H.323 Connection Capabilities” section on page 248.

4. Set up specific parameters for Cisco Unified CallManager. See the instructions in the “Enabling Interworking with Cisco Unified CallManager” section on page 249.

5. Set up dial peers to manage call legs within the network. See the “Setting Up Dial Peers” section on page 256.

Configuring Transfer and Forwarding Support

Note

Some of the commands in this section were introduced in Cisco CME 3.1 or later. To configure H.450 call transfer and forwarding on Cisco CME 3.0 systems, refer to the instructions in the Cisco CallManager Express 3.0 System Administrator Guide. For Cisco ITS V2.1 systems, refer to the Cisco IOS Telephony Services Version 2.1 guide.

The **transfer-system** command specifies the method to use for call transfers: H.450.2 standard signaling or Cisco proprietary signaling, and whether transfers should be blind or allow consultation. Cisco recommends that customers should specify H.450 standards for call transfer and forwarding when possible. For Cisco CME 4.0 and later versions, selection of the H.450.2 standard for call transfer is the default selection (the **full-consult** keyword is the default for the **transfer-system** command). However, prior to Cisco CME 4.0, the default was the Cisco proprietary method. Table 22 summarizes transfer method recommendations for all Cisco Unified CME versions.

Customers using a version of Cisco CME between 3.0 and 3.3 must configure the **transfer-system** command using the **full-consult** or **full-blind** keyword to allow IP phones to perform consultative or blind transfers to local phones and phones across a WAN. Note that prior to Cisco Unified CME 4.0, the default for the **transfer-system** command was the **blind** keyword, so the **transfer-system** command must be explicitly configured to use the recommended full-consult or full-blind setting.

Customers running Cisco IOS Telephony Services (Cisco ITS) 2.1 or an earlier version should use the **local-consult** or **blind** keyword with the **transfer-system** command to enable the Cisco proprietary transfer method.

Customers using Cisco ITS 2.1 can use the **full-consult** or **full-blind** keyword to enable H.450.2 call transfer by also configuring the router with a Tcl script that is contained in the file called app-h450-transfer.x.x.x.x.zip. This file is posted on the Cisco Unified CME software download website at http://www.cisco.com/cgi-bin/tablebuild.pl/ip-iostsp. For configuration steps, see the Cisco IOS Telephony Services Version 2.1 guide.
Table 22 Transfer Method Recommendations

<table>
<thead>
<tr>
<th>Cisco Unified CME Version</th>
<th>transfer-system Command Default</th>
<th>transfer-system Command to Use</th>
<th>Transfer Method Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.0 and later versions</td>
<td>full-consult</td>
<td>full-consult or full-blind</td>
<td>Use H.450.2 for call transfer, which is the default for this version. You do not need to use the transfer-system command unless you want to use the full-blind or dss keyword. Optionally, you can use the proprietary Cisco method by using the transfer-system command with the blind or local-consult keyword.</td>
</tr>
<tr>
<td>3.0 to 3.3</td>
<td>blind</td>
<td>full-consult or full-blind</td>
<td>Use H.450.2 for call transfer. You must explicitly configure the transfer-system command with the full-consult or full-blind keyword because H.450.2 is not the default for this version. Optionally, you can use the proprietary Cisco method by using the transfer-system command with the blind or local-consult keyword.</td>
</tr>
<tr>
<td>2.1 to 3.0</td>
<td>blind</td>
<td>blind or local-consult</td>
<td>Use the Cisco proprietary method, which is the default for this version. You do not need to use the transfer-system command unless you want to use the local-consult keyword. Optionally, you can use H.450.2 for call transfer by using transfer-system command with the full-consult or full-blind keyword. You must also configure the router with a Tcl script that is contained in the file called app-h450-transfer.x.x.x.x.zip. This file is posted on the Cisco Unified CME software download website at <a href="http://www.cisco.com/cgi-bin/tablebuild.pl/ip-iostsp">http://www.cisco.com/cgi-bin/tablebuild.pl/ip-iostsp</a>. For configuration information, see the Cisco IOS Telephony Services Version 2.1 guide.</td>
</tr>
<tr>
<td>Earlier than 2.1</td>
<td>blind</td>
<td>blind</td>
<td>Use the Cisco proprietary method, which is the default for this version. You do not need to use the transfer-system command unless you want to use the local-consult keyword.</td>
</tr>
</tbody>
</table>

The following configuration instructions are contained in this section:

- Enabling or Disabling H.450.2 and H.450.3 Capabilities, page 240
- Enabling or Disabling H.450.12 Capabilities, page 245
- Enabling H.323-to-H.323 Connection Capabilities, page 248
- Enabling Interworking with Cisco Unified CallManager, page 249
- Forwarding Calls from Cisco Unified CallManager to Cisco Unity Express Using Local Hairpin Routing, page 254
- Setting Up Dial Peers, page 256
- Verifying Transfer and Forwarding Support, page 256
Enabling or Disabling H.450.2 and H.450.3 Capabilities

H.450.2 is a standard protocol for exchanging call-transfer information across a network, whereas H.450.3 is a standard protocol for exchanging call-forwarding information across a network. The H.450.2 and H.450.3 standards are supported by Cisco CME 3.1 or later, Cisco CME 3.0, and Cisco ITS V2.1. The H.450.2 and H.450.3 standards are not supported by Cisco Unified CallManager, Cisco BTS, or Cisco PGW.

H.450.2 and H.450.3 capabilities are enabled by default for transferred or forwarded parties and transfer-destination or forward-destination parties. To enable H.450 call transfers and forwards for transferring or forwarding parties (that is, to allow transfers and forwards to be initiated from a Cisco Unified CME system), use the `transfer-system`, `transfer-pattern`, and `call-forward` pattern commands. Note that earlier versions of Cisco Unified CME handle transfers differently than later versions, and that the default for the `transfer-system` command was changed in Cisco Unified CME version 4.0. Table 22 presents recommendations for selecting a transfer method for all Cisco Unified CME versions.

The remaining commands in this task (supplementary-service h450.2 and supplementary-service h450.3) enable or disable H.450.2 and H.450.3 capabilities for transferred or forwarded parties and transfer-destination or forward-destination parties. Because these capabilities are enabled by default, these commands are normally required only if you want to explicitly disable H.450.2 or H.450.3 capabilities, either globally or on specific dial peers.

**SUMMARY STEPS**

1. telephony-service
2. transfer-system {blind | full-blind | full-consult [dss] | local-consult}
3. transfer-pattern transfer-pattern [blind]
4. call-forward pattern pattern
5. exit
6. voice service voip
7. supplementary-service h450.2
8. supplementary-service h450.3
9. exit
10. dial-peer voice tag voip
11. supplementary-service h450.2
12. supplementary-service h450.3
13. exit

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>telephony-service</td>
<td>Enters telephony-service configuration mode.</td>
</tr>
</tbody>
</table>

Example:

```
Router(config)# telephony-service
```
## Configuring Transfer and Forwarding Support

### Step 2

**Command or Action**

```
transfer-system {blind | full-blind | full-consult [dss] | local-consult}
```

**Example:**

```
Router(config-telephony)# transfer-system
full-consult
```

- **Purpose:** Specifies call transfer method.

  For H.323 networks and Cisco CME 3.0 or later, use only the `full-blind` or `full-consult` keyword. For Cisco CME versions from 3.0 to 3.3, you must explicitly configure the `full-consult` or `full-blind` keyword to use H.450 standards. For Cisco ITS 2.1 and earlier versions, use the `local-consult` or `blind` keyword. (Cisco ITS 2.1 can use the `full-blind` or `full-consult` keyword by also using the Tcl script in the file called `app-h450-transfer.x.x.x.x.zip`.)

  For SIP networks, use only the `full-blind` or `full-consult` keyword. For more information about SIP, refer to “SIP Trunk Features” section on page 275 in this guide and to the *Cisco IOS SIP Configuration Guide*.

- **Note:** The default for this command in Cisco Unified CME 4.0 and later versions is the `full-consult` keyword. For earlier versions, the default is the `blind` keyword.

- **blind**—Calls are transferred without consultation with a single phone line using the Cisco proprietary method. For Cisco CME versions earlier than 4.0, this is the default.

- **full-blind**—Calls are transferred without consultation using H.450.2 standard methods.

- **full-consult**—Calls are transferred with consultation using H.450.2 standard methods and a second phone line if available. The calls fall back to full-blind if the second line is unavailable. For Cisco Unified CME 4.0 and later versions, this is the default.

- **dss**—Calls are transferred with consultation to idle monitor lines. All other call-transfer behavior is identical to full-consult.

- **local-consult**—Calls are transferred with local consultation using a second phone line if available. The calls fall back to blind for nonlocal consultation or nonlocal transfer target.
### Configuring Transfer and Forwarding Support

#### Command or Action

<table>
<thead>
<tr>
<th>Step 3</th>
<th>transfer-pattern transfer-pattern [blind]</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Allows transfer of telephone calls by Cisco Unified IP phones to specified phone number patterns. If no transfer pattern is set, the default is that transfers are permitted only to other local IP phones.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• transfer-pattern—String of digits for permitted call transfers. Wildcards are allowed. A pattern of .T transfers all calling parties using the H.450.2 standard.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• blind—(Optional) When H.450.2 consultative call transfer is configured, forces transfers that match the pattern specified in this command to be executed as blind transfers. Overrides settings made using the transfer-system and transfer-mode commands.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> When defining transfers to nonlocal numbers, it is important to note that transfer-pattern digit matching is performed before translation-rule operations. Therefore, you should specify in this command the digits actually entered by phone users before they are translated. For more information, see the “Voice Translation Rules and Profiles” section on page 117.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 4</th>
<th>call-forward pattern pattern</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Specifies the H.450.3 standard for call forwarding. Calling-party numbers that do not match the patterns defined with this command are forwarded using Cisco proprietary call forwarding for backward compatibility, as described in the “Configuring Call Forwarding” chapter in the Cisco IOS Telephony Services Version 2.1 guide.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• pattern—Digits to match for call forwarding using the H.450.3 standard. If an incoming calling-party number matches the pattern, it can be forwarded using the H.450.3 standard. A pattern of .T forwards all calling parties using the H.450.3 standard.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> When defining forwards to nonlocal numbers, it is important to note that pattern digit matching is performed before translation-rule operations. Therefore, you should specify in this command the digits actually entered by phone users before they are translated. For more information, see the “Voice Translation Rules and Profiles” section on page 117.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 5</th>
<th>exit</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Exits telephony-service configuration mode.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 6</th>
<th>voice service voip</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>(Optional) Enters voice-service configuration mode to establish global call transfer and forwarding parameters.</td>
<td></td>
</tr>
</tbody>
</table>

---

**Example:**

- **Router(config-telephony)# transfer-pattern .T**
- **Router(config-telephony)# call-forward pattern .T**
- **Router(config-telephony)# exit**
- **Router(config)# voice service voip**

---

**Cisco Unified CallManager Express System Administrator Guide**

[442]
### Command or Action

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 7 | `supplementary-service h450.2` | (Optional) Enables H.450.2 supplementary services capabilities exchange globally. This is the default. Use the `no` form of this command to disable H.450.2 capabilities globally. This command is also used in dial-peer configuration mode to affect a single dial peer.  
  - If this command is enabled globally and enabled on a dial peer, the functionality is enabled for the dial peer. This is the default.  
  - If this command is enabled globally and disabled on a dial peer, the functionality is disabled for the dial peer.  
  - If this command is disabled globally and either enabled or disabled on a dial peer, the functionality is disabled for the dial peer. |
| Step 8 | `supplementary-service h450.3` | (Optional) Enables H.450.3 supplementary services capabilities exchange globally. This is the default. Use the `no` form of this command to disable H.450.3 capabilities globally. This command is also used in dial-peer configuration mode to affect a single dial peer.  
  - If this command is enabled globally and enabled on a dial peer, the functionality is enabled for the dial peer. This is the default.  
  - If this command is enabled globally and disabled on a dial peer, the functionality is disabled for the dial peer.  
  - If this command is disabled globally and either enabled or disabled on a dial peer, the functionality is disabled for the dial peer. |
| Step 9 | `exit` | (Optional) Exits voice-service configuration mode. |
| Step 10 | `dial-peer voice tag voip` | (Optional) Enters dial-peer configuration mode. |

### Example:

- Step 7: `supplementary-service h450.2`
  ```
  Router(conf-voi-serv)#
  supplementary-service h450.2
  ```

- Step 8: `supplementary-service h450.3`
  ```
  Router(conf-voi-serv)#
  supplementary-service h450.3
  ```

- Step 9: `exit`
  ```
  Router(conf-voi-serv)# exit
  ```

- Step 10: `dial-peer voice tag voip`
  ```
  Router(config)# dial-peer voice 1 voip
  ```
### Configuring Transfer and Forwarding Support

#### Example

The following example sets all transfers and forwards that are initiated by a Cisco CME 3.1 or later system to use the H.450 standards, globally enables H.450.2 and H.450.3 capabilities, and disables those capabilities for dial peer 37. The **supplementary-service** commands under voice-service configuration mode are not necessary because these values are the default, but they are shown here for illustration.

**telephony-service**  
**transfer-system full-consult**  
**transfer-pattern .T**  
**call-forward pattern .T**  

**!**  
**voice service voip**  
**supplementary-service h450.2**  
**supplementary-service h450.3**  

**!**  
**dial-peer voice 37 voip**  
**destination-pattern 555....**  
**session target ipv4:10.5.6.7**  
**no supplementary-service h450.2**  
**no supplementary-service h450.3**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 11</strong></td>
<td>(Optional) Enables H.450.2 supplementary services capabilities exchange for an individual dial peer. This is the default. This command is also used in voice-service configuration mode to enable H.450.2 services globally.</td>
</tr>
<tr>
<td>supplementary-service h450.2</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-dial-peer)# no supplementary-service h450.2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• If this command is enabled globally and enabled on a dial peer, the functionality is enabled for the dial peer. This is the default.</td>
</tr>
<tr>
<td></td>
<td>• If this command is enabled globally and disabled on a dial peer, the functionality is disabled for the dial peer.</td>
</tr>
<tr>
<td></td>
<td>• If this command is disabled globally and either enabled or disabled on a dial peer, the functionality is disabled for the dial peer.</td>
</tr>
<tr>
<td><strong>Step 12</strong></td>
<td>(Optional) Enables H.450.3 supplementary services capabilities exchange for an individual dial peer. This is the default. This command is also used in voice-service configuration mode to enable H.450.3 services globally.</td>
</tr>
<tr>
<td>supplementary-service h450.3</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-dial-peer)# no supplementary-service h450.3</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• If this command is enabled globally and enabled on a dial peer, the functionality is enabled for the dial peer. This is the default.</td>
</tr>
<tr>
<td></td>
<td>• If this command is enabled globally and disabled on a dial peer, the functionality is disabled for the dial peer.</td>
</tr>
<tr>
<td></td>
<td>• If this command is disabled globally and either enabled or disabled on a dial peer, the functionality is disabled for the dial peer.</td>
</tr>
<tr>
<td><strong>Step 13</strong></td>
<td>(Optional) Exits dial-peer configuration mode.</td>
</tr>
<tr>
<td>exit</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-dial-peer)# exit</td>
<td></td>
</tr>
</tbody>
</table>
What to Do Next

If you are using H.450.12 capabilities in your network, see the instructions in the “Enabling or Disabling H.450.12 Capabilities” section on page 245.

If you are configuring hairpin call routing or routing to an H.450 tandem gateway, see the instructions in the “Enabling H.323-to-H.323 Connection Capabilities” section on page 248.

If you are setting up a network that includes a Cisco Unified CallManager, see the instructions in the “Enabling Interworking with Cisco Unified CallManager” section on page 249.

Set up dial peers using the instructions in the Dial Peer Configuration on Voice Gateway Routers guide.

Enabling or Disabling H.450.12 Capabilities

The H.450.12 call capabilities standard provides a means to advertise and discover H.450.2 and H.450.3 capabilities in voice gateway endpoints on a call-by-call basis. When H.450.12 is enabled, H.450.2 and H.450.3 services are disabled for call transfers and call forwards unless a positive H.450.12 indication is received from all the other VoIP endpoints involved in the call. If positive H.450.12 indications are received, the router uses the H.450.2 standard for call transfers and the H.450.3 standard for call forwarding. If a positive H.450.12 indication is not received, the router uses the alternative method that you have configured for call transfers and forwards, either hairpin call routing or an H.450 tandem gateway.

H.450.12 capabilities are disabled by default to minimize the risk of compatibility issues with other types of H.323 systems. This optional task allows you to enable H.450.12 capabilities globally or by individual dial peer.

Note that Cisco CME 3.0 does not provide H.450.12 indications for calls even though it supports the H.450.2 and H.450.3 standards. The supplementary-service h450.12 command with the advertise-only keyword is intended for use on Cisco CME 3.1 or later systems that are mixed in a network with Cisco CME 3.0 systems. This scenario is usually found when you are upgrading a network from Cisco CME 3.0 systems to Cisco CME 3.1 or later. When you use the advertise-only keyword, the Cisco CME 3.1 or later router sends out H.450.12 indications for the benefit of remote VoIP endpoints, but does not require H.450.12 responses and has H.450.2 and H.450.3 enabled for all calls (the default). When in advertise-only mode, Cisco CME 3.1 or later is still able to automatically detect Cisco Unified CallManager systems.

SUMMARY STEPS

1. voice service voip
2. supplementary-service h450.12 [advertise-only]
3. exit
4. dial-peer voice tag voip
5. supplementary-service h450.12
6. exit
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> voice service voip</td>
<td>(Optional) Enters voice service configuration mode to establish global call transfer and forwarding parameters.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# voice service voip</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> supplementary-service h450.12 [advertise-only]</td>
<td>(Optional) Enables H.450.12 supplementary services capabilities exchange globally. Use this command for call-by-call detection of H.450 capabilities when some endpoints in your mixed network are H.450-capable and other endpoints are not. This command is disabled by default.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(conf-voi-serv)# supplementary-service h450.12</td>
<td></td>
</tr>
<tr>
<td><strong>advertise-only</strong>—(Optional) Advertises H.450 capabilities to the remote end but does not require H.450.12 responses. Use this keyword when you have only Cisco CME 3.0 systems in your network in addition to Cisco CME 3.1 or later systems. This command is also used in dial-peer configuration mode to affect an individual dial peer.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>• If this command is enabled globally and enabled on a dial peer, the functionality is enabled for the dial peer.</td>
<td></td>
</tr>
<tr>
<td>• If this command is enabled globally and disabled on a dial peer, the functionality is enabled for the dial peer.</td>
<td></td>
</tr>
<tr>
<td>• If this command is disabled globally and enabled on a dial peer, the functionality is enabled for the dial peer.</td>
<td></td>
</tr>
<tr>
<td>• If this command is disabled globally and disabled on a dial peer, the functionality is disabled for the dial peer. This is the default.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> exit</td>
<td>(Optional) Exits voice-service configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(conf-voi-serv)# exit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> dial-peer voice tag voip</td>
<td>(Optional) Enters dial-peer configuration mode. Use this command to set up individual dial peers to override global settings.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# dial-peer voice 1 voip</td>
<td></td>
</tr>
</tbody>
</table>
### Command or Action

#### Step 5

**supplementary-service h450.12**

*(Optional) Enables H.450.12 supplementary services capabilities exchange for an individual dial peer. This command is disabled by default.*

This command is also used in voice-service configuration mode to enable H.450.12 services globally.

- If this command is enabled globally and enabled on a dial peer, the functionality is enabled for the dial peer.
- If this command is enabled globally and disabled on a dial peer, the functionality is enabled for the dial peer.
- If this command is disabled globally and enabled on a dial peer, the functionality is enabled for the dial peer.
- If this command is disabled globally and disabled on a dial peer, the functionality is disabled for the dial peer. This is the default.

#### Step 6

**exit**

*(Optional) Exits dial-peer configuration mode.*

**Example:**

```
Router(config-dial-peer)# exit
```

### Example

The following example globally disables H.450.12 capabilities and then enables them only on dial peer 24.

```
voice service voip
 no supplementary-service h450.12
!
dial-peer voice 24 voip
 destination-pattern 555....
 session target ipv4:10.5.6.7
 supplementary-service h450.12
```

### What to Do Next

If you are configuring hairpin call routing or routing to an H.450 tandem gateway, see the instructions in the “Enabling H.323-to-H.323 Connection Capabilities” section on page 248.

If you are setting up a network that includes a Cisco Unified CallManager, see the instructions in the “Enabling Interworking with Cisco Unified CallManager” section on page 249.

Set up dial peers using the instructions in the *Dial Peer Configuration on Voice Gateway Routers* guide.
Enabling H.323-to-H.323 Connection Capabilities

VoIP-to-VoIP connections permit the termination and reorigination of transferred and forwarded calls over the VoIP network. VoIP-to-VoIP connections are used for hairpin call routing and for H.450 tandem gateways. The only type of VoIP-to-VoIP connection that is supported by Cisco CME 3.1 or later is H.323-to-H.323 connection.

VoIP-to-VoIP connections are disabled on the router by default, and they must be explicitly enabled to make use of hairpin call routing or an H.450 tandem gateway. In addition, you must configure a mechanism to direct transferred or forwarded calls to the hairpin or the H.450 tandem gateway, using one of the following methods:

- Enable H.450.12 capabilities globally or on the routes that your transfers and forwards take. See the “Enabling or Disabling H.450.12 Capabilities” section on page 245.
- Explicitly disable H.450.2 and H.450.3 capabilities globally or on the routes that your transfers and forwards take. See the “Enabling or Disabling H.450.2 and H.450.3 Capabilities” section on page 240.

Restrictions

H.323-to-SIP hairpin call routing is supported only for Cisco Unity Express. For more information, refer to Integrating Cisco CallManager Express and Cisco Unity Express.

SUMMARY STEPS

1. voice service voip
2. allow-connections h323 to h323
3. exit

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> voice service voip</td>
<td>Enters voice service configuration mode to establish global call transfer and forwarding parameters.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# voice service voip</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> allow-connections h323 to h323</td>
<td>Enables VoIP-to-VoIP call connections. Use the no form of the command to disable VoIP-to-VoIP connections; this is the default.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(conf-voi-serv)# allow-connections h323 to h323</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> exit</td>
<td>Exits voice-service configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(conf-voi-serv)# exit</td>
<td></td>
</tr>
</tbody>
</table>
Example

The following example globally enables H.323-to-H.323 connections:

```
voice service voip
  allow-connections h323 to h323
```

What to Do Next

If you are setting up a network that includes a Cisco Unified CallManager, see the instructions in the “Enabling Interworking with Cisco Unified CallManager” section on page 249.

Set up dial peers to establish hairpin call routing or routing to an H.450 tandem gateway using the instructions in the *Dial Peer Configuration on Voice Gateway Routers* guide.

Enabling Interworking with Cisco Unified CallManager

When Cisco CME 3.1 or later and Cisco Unified CallManager are used in the same network, some additional configuration is necessary, as described in the following sections:

- Configuring Cisco CME 3.1 or Later to Interwork with Cisco Unified CallManager, page 250
- Configuring Cisco Unified CallManager to Interwork with Cisco CME 3.1 or Later, page 253

Figure 28 shows a network containing Cisco Unified CME and Cisco Unified CallManager systems.

---

**Figure 28** Network with Cisco Unified CME and Cisco Unified CallManager Systems

[Diagram of network with Cisco Unified CME and CallManager systems, including dial peers and media termination point (MTP).]
Configuring Cisco CME 3.1 or Later to Interwork with Cisco Unified CallManager

All of the Cisco IOS commands in this section are optional because they are set by default to work with Cisco Unified CallManager. They are included here only to explain how to implement optional capabilities or return nondefault settings to their defaults.

**SUMMARY STEPS**

1. voice service voip
2. h323
3. telephony-service ccm-compatible
4. h225 h245-address on-connect
5. exit
6. supplementary-service h225-notify cid-update
7. exit
8. voice class h323 tag
9. telephony-service ccm-compatible
10. h225 h245-address on-connect
11. exit
12. dial-peer voice tag voip
13. supplementary-service h225-notify cid-update
14. voice-class h323 tag
15. exit

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> voice service voip</td>
<td>Enters voice-service configuration mode to establish global parameters.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# voice service voip</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> h323</td>
<td>Enters H.323 voice-service configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(conf-voi-serv)# h323</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> telephony-service ccm-compatible</td>
<td>(Optional) Globally enables a Cisco CME 3.1 or later system to detect a Cisco Unified CallManager and exchange calls with it. This is the default.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(conf-serv-h323)# telephony-service ccm-compatible</td>
<td>• Use the no form of the command to disable Cisco Unified CallManager detection and exchange. Using the no form of the command is not recommended. • Using this command in an H.323 voice class definition allows you to specify this behavior for an individual dial peer.</td>
</tr>
</tbody>
</table>
### Command or Action | Purpose
--- | ---
**Step 4**  
**h225 h245-address on-connect**  
**Example:**  
Router(conf-serv-h323)# h225 h245-address on-connect  
(Optional) Globally enables a delay for the H.225 message exchange of an H.245 transport address until a call is connected. The delay allows the Cisco Unified CallManager to generate local ringback for calls to Cisco Unified CME phones. This is the default.  
- The **no** form of this command disables the delay. Using the **no** form of the command is not recommended.  
- Using this command in an H.323 voice class definition allows you to specify this behavior for an individual dial peer.

**Step 5**  
**exit**  
**Example:**  
Router(conf-serv-h323)# exit  
Exits H.323 voice-service configuration mode.

**Step 6**  
**supplementary-service h225-notify cid-update**  
**Example:**  
Router(conf-voi-serv)# supplementary-service h225-notify cid-update  
(Optional) Globally enables H.225 messages with caller-ID updates to be sent to Cisco Unified CallManager. This is the default.  
- The **no** form of the command disables caller-ID update. Using the **no** form of the command is not recommended.  
This command is also used in dial-peer configuration mode to affect a single dial peer.  
- If this command is enabled globally and enabled on a dial peer, the functionality is enabled for that dial peer. This is the default.  
- If this command is enabled globally and disabled on a dial peer, the functionality is disabled for that dial peer.  
- If this command is disabled globally and either enabled or disabled on a dial peer, the functionality is disabled for that dial peer.

**Step 7**  
**exit**  
**Example:**  
Router(config-voice-service)# exit  
Exits voice-service configuration mode.

**Step 8**  
**voice class h323 tag**  
**Example:**  
Router(config)# voice class h323 48  
(Optional) Creates a voice class that contains commands to be applied to one or more dial peers.

**Step 9**  
**telephony-service ccm-compatible**  
**Example:**  
Router(config-voice-class)# telephony-service ccm-compatible  
(Optional) When this voice class is applied to a dial peer, enables the dial peer to exchange calls with a Cisco Unified CallManager system. This is the default.  
- The **no** form of the command disables call exchange with Cisco Unified CallManager. Using the **no** form of the command is not recommended.
Configuring Transfer and Forwarding Support

**What to Do Next**

Set up Cisco Unified CallManager using the steps in the “Configuring Cisco Unified CallManager to Interwork with Cisco CME 3.1 or Later” section on page 253.

**Configuring Cisco Unified CallManager to Interwork with Cisco CME 3.1 or Later**

Set up a Cisco Unified CallManager that is intended to interwork with a Cisco Unified CME system using the following special steps in addition to the normal Cisco Unified CallManager configuration.

**SUMMARY STEPS**

1. Set Cisco Unified CallManager service parameters.
2. Configure the Cisco CME 3.1 or later system as an ICT in the Cisco Unified CallManager network.
3. Ensure that the Cisco Unified CallManager network uses an MTP.

---

### Command or Action | Purpose
--- | ---

**Step 10**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>h225 h245-address on-connect</code></td>
<td>(Optional) When this voice class is applied to a dial peer, enables the calls that use this dial peer to delay the exchange of H.225 messages that contain the H.245 transport address until calls are connected. The delay allows the playing of local ringback for calls from Cisco Unified CallManager. This is the default.</td>
</tr>
</tbody>
</table>

*Example:*

```plaintext
Router(config-voice-class)# h225 h245-address on-connect
```

- The `no` form of this command disables the delay. Using the `no` form of the command is not recommended.

**Step 11**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>exit</code></td>
<td>Exits voice-class configuration mode.</td>
</tr>
</tbody>
</table>

*Example:*

```plaintext
Router(config-voice-class)# exit
```

**Step 12**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>dial-peer voice tag voip</code></td>
<td>(Optional) Enters dial-peer configuration mode to set parameters for an individual dial peer.</td>
</tr>
</tbody>
</table>

*Example:*

```plaintext
Router(config)# dial-peer voice 28 voip
```

**Step 13**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>supplementary-service h225-notify cid-update</code></td>
<td>(Optional) Enables H.225 messages with caller-ID updates to Cisco Unified CallManager for a specific dial peer. This is the default.</td>
</tr>
</tbody>
</table>

*Example:*

```plaintext
Router(config-dial-peer)# no supplementary-service h225-notify cid-update
```

- The `no` form of the command disables caller-ID updates. Using the `no` form of the command is not recommended.

**Step 14**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>voice-class h323 tag</code></td>
<td>(Optional) Applies the previously defined voice class with the specified tag number to this dial peer.</td>
</tr>
</tbody>
</table>

*Example:*

```plaintext
Router(config-dial-peer)# voice-class h323 48
```

**Step 15**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>exit</code></td>
<td>Exits dial-peer configuration mode.</td>
</tr>
</tbody>
</table>

*Example:*

```plaintext
Router(config-dial-peer)# exit
```
DETAILED STEPS

**Step 1**  Set Cisco Unified CallManager service parameters. From Cisco Unified CallManager Administration, choose Service Parameters. Choose the Cisco Unified CallManager service, and make the following settings:

- Set the H323 FastStart Inbound service parameter to False.
- Set the Send H225 User Info Message service parameter to H225 Info for Ring Back.

**Step 2**  Configure the Cisco CME 3.1 system as an ICT in the Cisco Unified CallManager network. For information about different intercluster trunk types and configuration instructions, refer to the Cisco Unified CallManager documentation.

**Step 3**  Ensure that the Cisco Unified CallManager network uses an MTP. The MTP is required to provide DSP resources for transcoding and for sending and receiving G.729 calls to the Cisco CME 3.1 or later system. All media streams between Cisco Unified CallManager and Cisco CME 3.1 or later must pass through the MTP because Cisco CME 3.1 does not support transcoding. For more information, refer to the Cisco Unified CallManager documentation.

**Step 4**  Set up dial peers to establish routing using the instructions in the *Dial Peer Configuration on Voice Gateway Routers* guide.

For more information about Cisco Unified CallManager, refer to the Cisco Unified CallManager documentation.

**Forwarding Calls from Cisco Unified CallManager to Cisco Unity Express Using Local Hairpin Routing**

When Cisco Unified CME is used to forward calls that originate on phones that do not support the H.450.3 standard (such as Cisco Unified CallManager phones), local hairpin routing must be used to forward the calls. For calling parties whose numbers match the pattern specified in the *call-forward pattern* command, the system automatically detects whether H.450.3 is supported and uses the appropriate method to forward calls.

In order to enable hairpin routing, the *allow connections* command must be used with the appropriate keywords (*h323* or *sip*) to denote the originating and terminating legs of the hairpin. To forward calls to Cisco Unity Express, connections must be allowed to a SIP trunk.

Optionally, you can explicitly disable the use of H.450.3 using the *no supplementary-service h450.3* command, but this is not required because the system automatically detects calls on which H.450.3 is not supported and local hairpin routing is required when the calling-party numbers match the pattern specified in the *call-forward pattern* command.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. telephony-service
4. call-forward pattern *pattern*
5. exit
6. voice service voip
7. allow connections from-type to to-type
8. [no] supplementary-service h450.3

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td>Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> telephony-service</td>
<td>Enters telephony-service configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# telephony-service</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> call-forward pattern pattern</td>
<td>Specifies the calling-party numbers for which to allow call forwarding with automatic detection of whether H.450.3 is supported. If H.450.3 is supported, H.450.3 is used for the forward and, if not, local hairpin is used.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-telephony)# call-forward pattern 6000</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> exit</td>
<td>Exits telephony-service configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-telephony)# exit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> voice service voip</td>
<td>Enters voice-service configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# voice service voip</td>
<td></td>
</tr>
</tbody>
</table>
Transfer and Forwarding Support

Configuring Transfer and Forwarding Support

Example

The following example sets up the ability to forward calls that originate from Cisco Unified CallManager phones and are routed through a Cisco Unified CME system to a Cisco Unity Express extension. Call forwarding is enabled for all calling parties, H.450.3 is disabled, and connections are allowed to SIP endpoints.

```
telephony-service
  call-forward pattern T

voice service voip
  no supplementary-service h450.3
  allow connections from h323 to sip
```

Setting Up Dial Peers

Dial peers describe the virtual interfaces to or from which a call is established. All voice technologies use dial peers to define the characteristics associated with a call leg. Attributes applied to a call leg include specific quality of service (QoS) features, compression/decompression (codec), voice activity detection (VAD), and fax rate. Dial peers are also used to establish the routing paths in your network, including special routing paths such as hairpins and H.450 tandem gateways. Set up dial peers using the instructions in the Dial Peer Configuration on Voice Gateway Routers guide.

Example

The following example shows dial peer 1001, which points to a Cisco Unified CallManager connection, and dial peer 1002, which is on the Cisco CME 3.1 or later router itself:

```
dial-peer voice 1001 voip
  description points-to-CCM
  destination-pattern 1.T
  codec g711ulaw
  session target ipv4:172.26.82.10
  allow connections from h323 to sip
```

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 7**

allow connections from-type to-type

Example:

Router(conf-voi-serv)# allow connections h323 to sip

| **Step 8**

supplementary-service h450.3

Example:

Router(conf-voi-serv)# no supplementary-service h450.3

(Optional) Enables H.450.3 supplementary services capabilities exchange globally. This is the default. Use the no form of this command to disable H.450.3 capabilities globally. This command can also be used in dial-peer configuration mode to disable H.450.3 functionality for a single dial peer.

**Note** If this command is disabled globally and either enabled or disabled on a dial peer, the functionality is disabled for the dial peer. |
dial-peer voice 1002 voip
description points to router
destination-pattern 4...
codec g711ulaw
session target ipv4:172.25.82.2

What to Do Next

After setting up dial peers and using the other appropriate commands in this chapter, you should be able to transfer and forward calls across your mixed network. Verify and troubleshoot the configuration as needed.

Verifying Transfer and Forwarding Support

Step 1

To verify the configuration, use the `show running-config` command. Output samples are located in the “Examples” section on page 256.

Examples

The following configuration examples are included in this section:

- Cisco CME 3.1 or Later and Cisco Unified CallManager in the Same Network: Example, page 257
- H.450 Tandem Gateway Working with Cisco CME 3.1 or Later and Cisco Unified CallManager: Example, page 259

Cisco CME 3.1 or Later and Cisco Unified CallManager in the Same Network: Example

The following example shows a running configuration for a Cisco CME 3.1 or later router that has a Cisco Unified CallManager in its network.

```
Router# show running-config

version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
enable password cisco
!
    aaa new-model
!
    aaa session-id common

no ip subnet-zero
!
ip dhcp pool phone1
    host 172.24.82.3 255.255.255.0
    client-identifier 0100.07eb.4629.9e
    default-router 172.24.82.2
    option 150 ip 172.24.82.2
    !
```
ip dhcp pool phone2
  host 172.24.82.4 255.255.255.0
  client-identifier 0100.0b5f.f932.58
  default-router 172.24.82.2
  option 150 ip 172.24.82.2

! ip cef
no ip domain lookup
no mpls ldp logging neighbor-changes
no ftp-server write-enable

! voice service voip
  allow-connections h323 to h323

! voice class codec 1
  codec preference 1 g711ulaw

! no voice hpi capture buffer
! no voice hpi capture destination

! interface FastEthernet0/0
  ip address 172.24.82.2 255.255.255.0
  duplex auto
d  
speed auto
h323-gateway voip interface
h323-gateway voip bind srcaddr 172.24.82.2

! ip classless
! ip route 0.0.0.0 0.0.0.0 172.24.82.1
! ip route 192.168.254.254 255.255.255.255 172.24.82.1

! ip http server
! tftp-server flash:P00303020700.bin

! voice-port 1/0/0

! voice-port 1/0/1

! dial-peer cor custom

! dial-peer voice 1001 voip
  description points-to-CCM
destination-pattern 1.T
  voice-class codec 1
  session target ipv4:172.26.82.10

! dial-peer voice 1002 voip
  description points_to_router
destination-pattern 4...
d  
voice-class codec 1
  session target ipv4:172.25.82.2

! dial-peer voice 1 pots
  destination-pattern 3000
  port 1/0/0

! dial-peer voice 1003 voip
  destination-pattern 26..
d  
  session target ipv4:22.22.22.38

!

telephony-service
  load 7960-7940 P00303020700
max-ephones 48
max-dn 15
ip source-address 172.24.82.2 port 2000
create cnf-files version-stamp Jan 01 2002 00:00:00
keepalive 10
max-conferences 4
moh minuet.au
transfer-system full-consult
transfer-pattern ....
!
ephone-dn 1
  number 3001
  name abcde-1
  call-forward busy 4001
!
ephone-dn 2
  number 3002
  name abcde-2
!
ephone-dn 3
  number 3003
  name abcde-3
!
ephone-dn 4
  number 3004
  name abcde-4
!
ephone 1
  mac-address 0003.EB27.289E
  button 1:1 2:2
!
ephone 2
  mac-address 000D.39F9.3A58
  button 1:3 2:4
!
line con 0
  exec-timeout 0 0
  logging synchronous
line aux 0
line vty 0 4
  password cisco
!
end

H.450 Tandem Gateway Working with Cisco CME 3.1 or Later and Cisco Unified CallManager: Example
The following example shows a sample configuration for a Cisco CME 3.1 or later system that is linked
to an H.450 tandem gateway that serves as a proxy for a Cisco Unified CallManager system.

Router# show running-config

Building configuration...

Current configuration : 1938 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker

Cisco Unified CallManager Express System Administrator Guide
258
enable password cisco

aaa new-model

aaa session-id common
no ip subnet-zero

ip cef
no ip domain lookup
no ftp-server write-enable
no scripting tcl init
no scripting tcl encdir

voice call send-alert

voice service voip
  allow-connections h323 to h323
  supplementary-service h450.12
  h323

voice class codec 1
  codec preference 1 g711ulaw
  codec preference 2 g729r8
  codec preference 3 g729br8

interface FastEthernet0/0
  ip address 172.27.82.2 255.255.255.0
duplex auto
speed auto

h323-gateway voip interface
  h323-gateway voip h323-id host24

ip classless
ip route 0.0.0.0 0.0.0.0 172.26.82.1
ip route 0.0.0.0 0.0.0.0 172.27.82.1
ip http server

dial-peer cor custom

  dial-peer voice 1001 voip
    description points-to-CCM
    destination-pattern 4...
    session target ipv4:172.24.89.150

  dial-peer voice 1002 voip
    description points to CCME1
    destination-pattern 28..
    session target ipv4:172.24.22.38

  dial-peer voice 1003 voip
    description points to CCME3
    destination-pattern 9...
    session target ipv4:192.168.1.29

  dial-peer voice 1004 voip
    description points to CCME2
    destination-pattern 29..
    session target ipv4:172.24.22.42

line con 0
  exec-timeout 0 0
logging synchronous
line aux 0
Troubleshooting Transfer and Forwarding Support

Step 1  If you encounter lack of ringback on direct calls from a Cisco Unified CallManager phone to an IP phone on a Cisco Unified CM E system, check the `show running-config` command output to make sure that the following two commands do not appear: `no h225 h245-address on-connect` and `no telephony-service ccm-compatible`. Both of these commands should be enabled, which is their default state.

Step 2  The `debug h225 asn1` command can be used to look at the H.323 messages that are being sent from the Cisco Unified CME system to the Cisco Unified CallManager system to see if the H.245 address is being sent too early.

Step 3  For calls that are routed using VoIP-to-VoIP connections, the `show voip rtp connections detail` command displays the call identification number, IP addresses, and port numbers involved for all VoIP call legs. This command includes VoIP-to-POTS and VoIP-to-VoIP call legs. The following is sample output for this command:

```
Router# show voip rtp connections detail
VoIP RTP active connections:
No. CallId dstCallld LocalRTP RmtRTP LocalIP RemoteIP
 1     7        8      16586     22346  172.27.82.2     172.29.82.2
 2     8        7      17010     16590  172.27.82.2     200.1.1.29
Found 2 active RTP connections
```  

Step 4  The `show call prompt-mem-usage detail` command shows information on ringback tone generation that uses the interactive voice response (IVR) prompt playback mechanism. This ringback is needed for hairpin transfers that are committed during the alerting-of-the-transfer-destination phase of the call and for calls to destinations that do not provide in-band ringback tone, such as IP phones (FXS analog ports do provide in-band ringback tone). Ringback tone is played to the transferred party by the Cisco Unified CME system that performs the transfer (the system attached to the transferring party). The system automatically generates tone prompts as needed based on the network-locale setting for the Cisco Unified CME system.

If you are not getting ringback tone when you should, use the `show call prompt-mem-usage` command to make sure that the correct prompt is loaded and playing. The following sample output indicates that a prompt is playing (“Number of prompts playing”) and indicates the country code used for the prompt (GB for Great Britain) and the codec.

```
Router# show call prompt-mem-usage detail
Prompt memory usage:
file(s) config'd wait active free mc total ms total
0200 0001 -001 00200 00001 00002
memory 02097152 00003000 00000000 02094152 00003900
Prompt load counts: (counters reset 0)
success 0(1st try) 0(2nd try), failure 0
Other mem block usage:
mcDynamic mcReader
gauge 00001 00000
Number of prompts playing: 1
Number of start delays : 0
MCs in the ivr MC sharing table
```
Feature History for Transfer and Forwarding Support

<table>
<thead>
<tr>
<th>Cisco Unified CME Version</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>Call transfer was introduced, using a Cisco proprietary method. Call forwarding for all calls, busy conditions, and no-answer conditions was introduced, using a Cisco proprietary method.</td>
</tr>
<tr>
<td>2.1</td>
<td>Support was introduced for consultative transfer using the ITU-T H.450.2 standard. Support was introduced for the H.450.3 standard method for call forwarding.</td>
</tr>
</tbody>
</table>
| 3.0                       | • Local hairpin call routing was supported as an option for networks that cannot support H.450 call transfer and forwarding. This feature requires installation of the Tcl script app_h450_transfer.2.0.0.8.tcl or a later version.  
  • The CFwdALL (call-forward all) soft key was introduced. |
| 3.1                       | • Support was introduced for the following:  
  − Enhancements for VoIP networks which contain a mix of platforms that support H.450.2 and H.450.3 standards, such as Cisco CME 3.1, Cisco CME 3.0, Cisco ITS V2.1, and platforms that do not support H.450.2 and H.450.3 standards, such as Cisco Unified CallManager, Cisco BTS Softswitch (BTS), and Cisco PSTN Gateway (PGW).  
  − H.450.12 standards.  
  − Automatic detection of Cisco Unified CallManager endpoints.  
  − Hairpin VoIP-to-VoIP call routing and routing to an H.450 tandem gateway.  
  • The number of digits that can be entered using the CfwdALL soft key on an IP phone can be limited. |
Transfer and Forwarding Support

Related Features

<table>
<thead>
<tr>
<th>Related Features</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Call Forwarding</strong></td>
</tr>
<tr>
<td>Instructions for configuring call forwarding for individual ephone-dns is provided in the “Call Forwarding” section on page 372.</td>
</tr>
</tbody>
</table>

| **Call Transfer** |
| Instructions for configuring call-transfer features are provided in the “Call Transfer” section on page 465. |

### Cisco Unified CME Version Modification

<table>
<thead>
<tr>
<th>Cisco Unified CME Version</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.2</td>
<td>Consultative transfer to monitored lines using direct station select was introduced.</td>
</tr>
<tr>
<td>4.0</td>
<td>- The default for the <strong>transfer-system</strong> command was changed from the <strong>blind</strong> keyword to the <strong>full-consult</strong> keyword.</td>
</tr>
<tr>
<td></td>
<td>- The ability to transfer calls to phones outside the Cisco Unified CME system can be blocked for individual ephones.</td>
</tr>
<tr>
<td></td>
<td>- The number of digits in transfer destination numbers can be limited.</td>
</tr>
<tr>
<td></td>
<td>- Automatic call forwarding during night service was introduced.</td>
</tr>
<tr>
<td></td>
<td>- Selective call forwarding was introduced.</td>
</tr>
<tr>
<td></td>
<td>- The forwarding of local (internal) calls can be blocked.</td>
</tr>
</tbody>
</table>
Trunking Support

Trunking support features provide or enhance different types of trunk services. This chapter describes the following topics:

- Direct FXO Trunk Lines, page 264
- QSIG Supplementary Services, page 270
- SIP Trunk Features, page 275

Note


Trunking Support Overview

Trunking support features provide or enhance trunk services from Cisco Unified CME to other call-control devices in the PSTN or VoIP network. Table 23 summarizes trunking support features.

Table 23  Trunking Support Features

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Benefit</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Direct FXO Trunk Lines</td>
<td>System creates a private-line automatic ringdown off-premise extension for</td>
<td>Phone user makes and receives calls without going through Cisco Unified</td>
<td>A sales manager has a direct FXO trunk line with a number that is local</td>
</tr>
<tr>
<td></td>
<td>direct connection to a PSTN central office.</td>
<td>CME and has a number provided by the PSTN.</td>
<td>to most company clients, and has another line on the phone that is a</td>
</tr>
<tr>
<td>QSIG Supplementary Services</td>
<td>System enables H.450 supplementary services for QSIG interworking.</td>
<td>System administrator can interface Cisco Unified CME system to PBX or</td>
<td>Phone users have access to PBX applications.</td>
</tr>
<tr>
<td>SIP Trunk Features</td>
<td>System enables functionality that is necessary to interwork with SIP</td>
<td>System administrator can interface Cisco Unified CME system to SIP</td>
<td>Phone users can make calls and use some features across SIP networks.</td>
</tr>
<tr>
<td></td>
<td>networks.</td>
<td>networks.</td>
<td></td>
</tr>
</tbody>
</table>
Direct FXO Trunk Lines

Direct FXO trunk lines provide phone users direct access to a PSTN central office line. This section describes the following topics:

- Direct FXO Trunk Lines Overview, page 264
- Configuring Direct FXO Trunk Lines, page 266
- Verifying Direct FXO Trunk Lines, page 269
- Examples, page 269
- Feature History for Direct FXO Trunk Lines, page 270

Direct FXO Trunk Lines Overview

For a summary of the functionality introduced in different releases, see the “Feature History for Direct FXO Trunk Lines” section on page 270.

For Cisco CME3.2 and later versions, IP phones can be configured to have buttons for dedicated FXO trunk lines, hereinafter referred to as FXO lines. Direct FXO trunk lines may be used by companies whose employees require private PSTN numbers. For example, a salesperson may need a special number that customers can call without having to go through a main number. When a call comes in to the direct number, the salesperson knows that the caller is a customer. In the salesperson’s absence the customer can leave voice mail. Dedicated lines can use PSTN service provider voice mail: when the line button is pressed, the PSTN-FXO line is seized, allowing the user to hear the stutter dial tone provided by the PSTN to indicate that voice messages are available.

Because dedicated FXO lines behave as private lines, users do not have to dial a prefix, such as 9 or 8, to reach an outside line. To reach phone users within the company, FXO-line users must dial numbers that use the company’s PSTN number. For calls to non-PSTN destinations, such as local IP phones, a second ephone-dn must be provisioned.

Calls placed to or received on an FXO line have restricted Cisco Unified CME services (see the “Restrictions” section on page 265) and cannot be transferred by Cisco Unified CME. However, phone users are able to access hookflash-controlled PSTN services using the Flash soft key. Refer to the fxo hook-flash command in the Cisco Unified CallManager Express Command Reference.

From a high level, configuration of a direct FXO trunk line consists of the following:

1. Configuring the FXO port for a private line automatic ringdown (PLAR) off-premises extension (OPX) connection and declaring a private line’s number; for example:

   voice-port 1/1/0
   connection plar-opx 1020

2. Configuring dial peers for FXO port and declaring a trunk tag to bind the FXO port and its dial peer to an ephone-dn; for example:

   dial-peer voice 111 pots
destination-pattern 82
port 1/1/0
3. Configuring the ephone-dn and ephone; for example:

```plaintext
ephone-dn 12
  number 1020
```

```plaintext
ephone-dn 1
  mac-address 1111.1111.1111
  button 1:12
```

4. Binding the ephone-dn to the FXO port with the `trunk` command; for example:

```plaintext
ephone-dn 12
  number 1020
  trunk 82 timeout 30
```

The `trunk` command’s `timeout seconds` keyword and argument control the amount of time that Cisco Unified CME waits to collect digits for the dialed number, for the purpose of inclusion of the digits in the redial buffer and the Placed Calls directory of the phone. Digits that are entered after the timeout period are not included in the redial buffer or in the Placed Calls directory on the phone. The timeout parameter does not affect the time used to cut through the connection from the phone’s trunk button to the FXO port.

The phone user also has the option to use the phone’s on-hook dialing feature so that the phone itself performs complete dial-string digit collection before signaling offhook to the Cisco Unified CME router. In this case all digits will be included in the Redial and Placed Calls Directory.

### Restrictions

- An ephone-dn with a trunk line cannot be configured for call forward, busy, or no answer.
- An ephone-dn with a trunk line can be configured only as a single-line ephone-dn.
- Numbers entered after a trunk line is seized will not be displayed. Only the trunk tag is displayed on IP phones.
- Numbers entered after trunk line is seized will not appear in call history or call detail records (CDRs) of a Cisco Unified CME router. Only the trunk tag will be logged for calls made from trunk lines.
- FXO trunk lines do not support the CFwdALL, Transfer, Pickup, GPickUp, Park, CallBack, and NewCall soft keys.
- FXO trunk lines do not support conference initiator dropoff.
- FXO trunk lines do not support on-hook redial. The phone user must explicitly select the FXO trunk line before pressing the Redial button.
- FXO trunk lines do not support call transfer to IP phones. However, the call initiator can conference an FXO line with an IP phone by pressing the Hold button, which leaves the FXO trunk line and IP phone connected. The conference initiator is unable to participate in the conference, but can place calls on other lines.
Configuring Direct FXO Trunk Lines

This procedure sets up a direct FXO trunk line on an IP phone.

SUMMARY STEPS

1. enable
2. configure terminal
3. voice-port {slot-number/subunit-number/port | slot/port:ds0-group-number}
4. connection plar-opx digits
5. exit
6. dial-peer voice tag pots
7. destination-pattern [+ string [T]]
8. port {slot-number/subunit-number/port | slot/port:ds0-group-number}
9. exit
10. ephone-dn dn-tag
11. number number
12. trunk digit-string timeout seconds
13. exit
14. ephone phone-tag
15. mac-address tag
16. button button-number{separator}dn-tag [[button-number{separator}dn-tag] ...]
17. exit

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
</tbody>
</table>

**Step 2** configure terminal

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong> Router# configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>
### Command or Action

**Step 3**

```bash
voice-port {slot-number/subunit-number/port | slot/port:ds0-group-number}
```

**Example:**

```
Router(config)# voice-port 0/0/0
```

- **Purpose:** Enters voice-port configuration mode.
- **Note:** The example shows a voice-port configuration for the Cisco 2600, Cisco 3600 series, and Cisco 7200 series. The syntax options for other platforms may vary. For more information, refer to the *Cisco IOS Voice Command Reference*.

**Step 4**

```bash
connection plar-opx digits
```

**Example:**

```
Router(config-voice-port)# connection plar-opx 5550111
```

- **Purpose:** Specifies a PLAR OPX connection.
  - Using this option, the local voice port provides a local response before the remote voice port receives an answer. On FXO interfaces, the voice port does not answer until the remote side has answered.
  - **digits**—Specifies the destination telephone number. Valid entries are any series of digits that specify the E.164 telephone number.

**Step 5**

```bash
exit
```

**Example:**

```
Router(config-voice-port)# exit
```

- **Purpose:** Exits voice-port configuration mode.

**Step 6**

```bash
dial-peer voice tag pots
```

**Example:**

```
Router(config)# dial-peer voice 53 pots
```

- **Purpose:** Enters dial-peer configuration mode for POTS.
  - **tag**—Digits that define a particular dial peer. Range is from 1 to 2147483647.

**Step 7**

```bash
destination-pattern [+] string [T]
```

**Example:**

```
Router(config-dial-peer)# destination-pattern 20
```

- **Purpose:** Declares a prefix, access code, or full E.164 telephone number (depending on your dial plan) to be used for a dial peer.

**Step 8**

```bash
port {slot-number/subunit-number/port | slot/port:ds0-group-number}
```

**Example:**

```
Router(config-dial-peer)# port 0/0/0
```

- **Purpose:** Associates a dial peer with a specific voice port.
- **Note:** The example shows a voice-port configuration for the Cisco 2600, Cisco 3600 series, and Cisco 7200 series. The syntax options for other platforms may vary. For more information, refer to the *Cisco IOS Voice Command Reference*.
  - Use the PLAR connection voice port configured by the **connection** command.

**Step 9**

```bash
exit
```

**Example:**

```
Router(config-ephone-template)# exit
```

- **Purpose:** Exits dial-peer configuration mode.
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 10**  
`ephone-dn tag`  
**Example:**  
`Router(config)# ephone-dn 1` | Enters ephone-dn configuration mode to create an extension (ephone-dn) for a Cisco Unified IP phone line, an intercom line, a paging line, a voice-mail port, or an MWI.  
- *tag*—Unique sequence number that identifies an ephone-dn during configuration tasks. Range is from 1 to the maximum number of ephone-dns allowed on the router platform. Refer to the command-line interface (CLI) help for the maximum value for this argument. |
| **Step 11**  
`number number`  
**Example:**  
`Router(config-ephone-dn)# number 5550111` | Associates a telephone or extension number with an extension (ephone-dn).  
- *number*—String of up to 16 characters that represents an E.164 telephone number. Enter the PLAR number configured by the `connection` command. |
| **Step 12**  
`trunk digit-string timeout seconds`  
**Example:**  
`Router(config-ephone-dn)# trunk 20 timeout 30` | Associates an ephone-dn with an FXO port's trunk number so the ephone-dn can support a direct FXO line.  
- *digit-string*—Declares the number of the trunk line. Use the `string` argument specified in the `destination-pattern` command.  
- *timeout seconds*—Sets the timeout between digits for dialing. The phone user has to either enter the pound (#) key or wait for the interdigit timeout to complete the digit dialing. Range is from 3 to 30. The default is 3. |
| **Step 13**  
`exit` | Exits ephone-dn configuration mode. |
| **Step 14**  
`ephone phone-tag`  
**Example:**  
`Router(config)# ephone 1` | Enters ephone configuration mode for an IP phone. |
| **Step 15**  
`mac-address mac-address`  
**Example:**  
`Router(config-ephone)# mac-address CFBA.321B.96FA` | Associates the MAC address of a Cisco Unified IP phone with an ephone configuration in a Cisco Unified CME system.  
- *mac-address*—The MAC address of an IP phone, which is found on a sticker located on the bottom of the phone. |
Verifying Direct FXO Trunk Lines

Step 1 Use the `show running-config` command to verify voice port, dial-peer, ephone-dn, and ephone parameters.

Examples

The following example shows the configuration for one phone that has 2 buttons: the first button is for making calls to local extensions and for receiving calls, and the second button is for a private line that goes out an FXO port as a direct trunk.

```
voice-port 1/0/0
connection plar opx 1001
dial-peer voice 100 pots
destination-pattern 81
voice-port 1/0/0
ephone-dn 1
name MainExtension
number 1001
ephone-dn 2
name PrivateTrunkLine
trunk 81 timeout 5
```
Feature History for Direct FXO Trunk Lines

<table>
<thead>
<tr>
<th>Cisco Unified CME Version</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.2</td>
<td>Direct FXO trunk line capability was introduced.</td>
</tr>
</tbody>
</table>

QSIG Supplementary Services

QSIG supplementary services allow Cisco Unified CME phones to use QSIG to interwork with PBX phones in a seamless fashion. This section describes the following topics:

- QSIG Supplementary Services Overview, page 270
- Configuring QSIG Supplementary Services, page 272
- Verifying QSIG Supplementary Services, page 274
- Examples, page 281
- Feature History for QSIG Supplementary Services, page 275

QSIG Supplementary Services Overview

Note For a summary of the functionality introduced in different releases, see the “QSIG Supplementary Services Overview” section on page 270.

QSIG is an intelligent inter-PBX signaling system widely adopted by PBX vendors. It supports a range of basic services, generic functional procedures, and supplementary services. Cisco Unified CME 4.0 introduces supplementary services features that allow Cisco Unified CME phones to seamlessly interwork using QSIG with phones connected to a PBX. One benefit is that IP phones can use a PBX message center with proper MWI notifications. Figure 29 illustrates a topology for a Cisco Unified CME system with some phones under the control of a PBX.
The following QSIG supplementary service features are supported in Cisco Unified CME systems. They follow the standards from the European Computer Manufacturers Association (ECMA) and the International Organization for Standardization (ISO) on PRI and BRI interfaces.

- Basic calls between IP phones and PBX phones.
- Calling Line/Name Identification (CLIP/CNIP) presented on an IP phone when called by a PBX phone; in the reverse direction, such information is provided to the called endpoint.
- Connected Line/Name Identification (COLP/CONP) information provided when a PBX phone calls an IP phone and is connected; in the reverse direction, such information presented on an IP phone.
- Call Forward using QSIG and H.450.3 to support any combination of IP phone and PBX phone, including an IP phone in the Cisco Unified CME system that is connected to a PBX or an IP phone in another Cisco Unified CME system across an H.323 network.
- Call forward to the PBX message center according to the configured policy. The other two endpoints can be a mixture of IP phone and PBX phones.
- Hairpin call transfer, which interworks with a PBX in transfer-by-join mode. Note that Cisco Unified CME does not support the actual signaling specified for this transfer mode (including the involved FACILITY message service APDUs) which are intended for an informative purpose only and not for the transfer functionality itself. As a transferrer (XOR) host, Cisco Unified CME simply hairpins two call legs to create a connection; as a transferee (XEE) or transfer-to (XTO) host, it will not be aware of a transfer that is taking place on an existing leg. As a result, the final endpoint may not be updated with the accurate identity of its peer. Both blind transfer and consult transfer are supported.
- Message-waiting indicator (MWI) activation or deactivation requests are processed from the PBX message center.
- The PBX message center can be interrogated for the MWI status of a particular ephone-dn.
- A user can retrieve voice messages from a PBX message center by making a normal call to the message center access number.
Configuring QSIG Supplementary Services

This procedure enables QSIG supplementary services.

SUMMARY STEPS

1. enable
2. configure terminal
3. telephony-service
4. voicemail phone-number
5. transfer-system { blind | full-blind | full-consult | local-consult }
6. exit
7. ephone-dn dn-tag
8. mwi qsig
9. Configure call forwarding to the voice-mail number for this ephone-dn.
10. exit
11. voice service voip
12. supplementary-service h450.7
13. exit
14. supplementary-service qsig call-forward

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Router&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3 telephony-service</td>
<td>Enters telephony-service configuration mode.</td>
</tr>
<tr>
<td>Example: Router(config)# telephony-service</td>
<td></td>
</tr>
<tr>
<td>Step 4 voicemail phone-number</td>
<td>Specifies a directory number for voice mail. The PBX message center number can be entered here.</td>
</tr>
<tr>
<td>Example: Router(config-telephony)# voicemail 74398</td>
<td>Note: Be sure to configure a POTS dial peer and an ISDN interface for the message center line.</td>
</tr>
</tbody>
</table>
Step 5  

**Command or Action:**  
`transfer-system {blind | full-blind | full-consult | local-consult}`

**Example:**  
Router(config-telephony)# transfer-system  
full-consult

**Purpose:** Defines the call transfer method to allow call transfer with consultation for all lines served by the router.

**Note**  
For SIP networks, use only the **full-blind** keyword or the **full-consult** keyword.

- **blind**—Calls are transferred without consultation with a single phone line using the Cisco-proprietary method.
- **full-blind**—Calls are transferred without consultation using H.450.2 standard methods.
- **full-consult**—Calls are transferred with consultation using H.450.2 standard methods and a second phone line if available. The calls fall back to full-blind if the second line is unavailable.
- **local-consult**—Calls are transferred with local consultation using a second phone line if available. The calls fall back to blind for nonlocal consultation or nonlocal transfer target.

**Step 6**  

**Command or Action:**  
`exit`

**Example:**  
Router(config-telephony)# exit

**Purpose:** Exits telephony-service configuration mode.

**Step 7**  

**Command or Action:**  
`ephone-dn dn-tag`

**Example:**  
Router(config)# ephone-dn 25

**Purpose:** Enters ephone-dn configuration mode.

- **dn-tag**—Unique sequence number that identifies this ephone-dn during configuration tasks.

**Step 8**  

**Command or Action:**  
`mwi qsig`

**Example:**  
Router(config-ephone-dn)# mwi qsig

**Purpose:** Specifies that the QSIG (PBX) message center should be interrogated for MWI status for this ephone-dn.

**Step 9**  

**Command or Action:**  
Configure call forwarding to the voice-mail number for this ephone-dn.

**Example:**  
Router(config-ephone-dn)# exit

**Step 10**  

**Command or Action:**  
`exit`

**Example:**  
Router(config-ephone-dn)# exit

**Purpose:** Exits ephone-dn configuration mode.
<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td><code>voice service voip</code></td>
<td>Enters VoIP voice-service configuration mode to establish global call transfer and forwarding parameters.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Router(config)# voice service voip</code></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td><code>supplementary-service h450.7</code></td>
<td>Enables H.450.7 supplementary services capabilities exchange globally. This command is disabled by default.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Router(config-voi-serv)# supplementary-service h450.7</code></td>
<td>Note: Use this command in voice-service configuration mode to enable H.450.7 supplementary services globally, or in dial-peer configuration mode to enable the services on a single dial peer.</td>
</tr>
<tr>
<td>13</td>
<td><code>exit</code></td>
<td>Exits VoIP voice-service configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Router(config-voi-serv)# exit</code></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td><code>voice service pots</code></td>
<td>Enters POTS voice-service configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Router(config)# voice service pots</code></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td><code>supplementary-service qsig call-forward</code></td>
<td>Provides QSIG call-forwarding supplementary services (ISO 13873) when necessary to forward calls to another number. This command is disabled by default.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Router(config-voi-serv)# supplementary-service qsig call-forward</code></td>
<td>Note: Use this command in voice-service configuration mode to enable QSIG call-forwarding services globally, or in dial-peer configuration mode to enable the services on a single dial peer.</td>
</tr>
</tbody>
</table>

**Verifying QSIG Supplementary Services**

**Step 1**

Use the `show running-config` command to display telephony-service, ephone-dn, and voice-service settings.

---

**Examples**

The following example implements QSIG supplementary services on extension 74367 and globally enables H.450.7 supplementary services and QSIG call-forwarding supplementary services.

```plaintext
telephony-service
  voicemail 74398
  transfer-system full-consult

  ephone-dn 25
  number 74367
  mwi qsig
  call-forward all 74000
```
Feature History for QSIG Supplementary Services

<table>
<thead>
<tr>
<th>Cisco Unified CME Version</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.0</td>
<td>QSIG supplementary services capability was introduced.</td>
</tr>
</tbody>
</table>

SIP Trunk Features

SIP trunk features enable interoperability between Cisco Unified CME phones and SIP networks. This section describes the following topics:

- SIP Trunk Features Overview, page 275
- Configuring SIP Trunk Support, page 277
- Verifying SIP Trunk Support Features, page 280
- Examples, page 281
- Troubleshooting SIP Trunk Support Features, page 282
- Feature History for SIP Trunk Features, page 283
- Related Features, page 283

SIP Trunk Features Overview

Note

For a summary of the functionality introduced in different releases, see the “SIP Trunk Features Overview” section on page 275.

When Cisco Unified CME and SCCP phones are used with SIP networks, the following features may need special settings:

- Call Forwarding over SIP Networks, page 276
- Call Transfer over SIP Networks, page 276
- DTMF Relay, page 276
- SIP Register Support, page 277
Call Forwarding over SIP Networks

Call forwarding over SIP networks uses the 302 Moved Temporarily SIP response, which works in a manner similar to the way in which the H.450.3 standard is used for H.323 networks. To enable call forwarding, use the call-forward pattern command and specify a pattern that matches the calling-party numbers of the calls that you want to be able to forward. Use the call-forward pattern command with the .T pattern to allow all calls for all possible SIP calling parties to be forwarded using the SIP 302 response.

Call Transfer over SIP Networks

Cisco Unified CME supports all SIP Refer method call transfer scenarios, but you must be sure that call transfer is enabled using H.450.2 standards. Note that the transfer-system command must be configured with the full-blind or full-consult keyword for SIP Refer to be invoked.

DTMF Relay

SCCP phones used with Cisco Unified CME systems relay dual tone multifrequency (DTMF) digits out of band. To interwork with SIP applications that expect in-band DTMF digits, you must enable a conversion. Two types of conversions are possible:

- RFC 2833 (Standard) DTMF Relay—for remote SIP-based IVR or voice-mail application
- SIP Notify (Nonstandard) DTMF Relay—for Cisco Unity Express on a SIP network

RFC 2833 (Standard) DTMF Relay
To use remote voice-mail or interactive voice response (IVR) applications on SIP networks from Cisco Unified CME phones, you must enable conversion of the out-of-band dual tone multifrequency (DTMF) digits used by the Cisco Unified CME phones to the RFC 2833 in-band DTMF relay mechanism used by SIP phones. You select this method in the SIP VoIP dial peer using the dtmf-relay rtp-nte command.

The SIP DTMF relay method is needed in the following situations:

- When SIP is used to connect a Cisco Unified CME system to a remote SIP-based IVR or voice-mail application.
- When SIP is used to connect a Cisco Unified CME system to a remote SIP-PSTN voice gateway that goes through the PSTN to a voice-mail or IVR application.

Note that the need to use out-of-band DTMF relay conversion is limited to SCCP phones. SIP phones natively support in-band DTMF relay as specified in RFC 2833.

To enable SIP DTMF relay using RFC2833, the commands in this section must be used on both originating and terminating gateways.

SIP Notify (Nonstandard) DTMF Relay
To use voice mail on a SIP network that connects to a Cisco Unity Express system, use a non-standard SIP Notify format. To configure the Notify format, use the sip-notify keyword with the dtmf-relay command. Using the keyword sip-notify may be required for backward compatibility with Cisco CME Versions 3.0 and 3.1.
SIP Register Support

SIP register support enables a SIP gateway to register E.164 numbers with a SIP proxy or SIP registrar, similar to the way that H.323 gateways can register E.164 numbers with a gatekeeper. SIP gateways allow registration of E.164 numbers to a SIP proxy or registrar on behalf of analog telephone voice ports (FXS) and IP phone virtual voice ports (EFXS) for local SCCP phones. This support is enabled using the `register` command in SIP UA configuration mode.

When registering E.164 numbers in dial peers with an external registrar, you can also register them with a secondary SIP proxy or registrar to provide redundancy. The secondary registration can be used if the primary registrar fails.

For more detailed information, refer to *SIP Gateway Enhancements*, Cisco IOS Release 12.2(15)ZJ.

**Note**

There are no commands that allow registration between the H.323 and SIP protocols.

By default, SIP gateways do not generate SIP Register messages, so the following steps are needed to set up the gateway to register the gateway’s E.164 telephone numbers with an external SIP registrar.

Configuring SIP Trunk Support

This procedure enables four SIP trunk support parameters:

- Call forwarding over SIP networks—`call-forward pattern` and `calling-number local` commands
- Call transfer over SIP networks—`transfer-system` and `transfer-pattern` commands
- DTMF relay—`dtmf-relay rtp-nte` or `dtmf-relay sip-notify` command and `notify telephone-event max-duration` command
- SIP registrar—`registrar`, `retry`, and `timers` commands

**SUMMARY STEPS**

1. enable
2. configure terminal
3. telephony-service
4. call-forward pattern pattern
5. calling-number local
6. transfer-system {full-blind | full-consult}
7. transfer-pattern transfer-pattern
8. exit
9. dial-peer voice tag voip
10. dtmf-relay rtp-nte
11. dtmf-relay sip-notify
12. exit
13. sip-ua
14. notify telephone-event max-duration time
15. `registrar {dns:host-name | ipv4:ip-address} expires seconds [tcp] [secondary]

16. `retry register number

17. `timers register time

18. `exit

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> <code>enable</code></td>
<td>- Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> <code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> telephony-service</td>
<td>Enters telephony-service configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> <code>telephony-service</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> <code>call-forward pattern pattern</code></td>
<td>Specifies the H.450.3 standard or SIP 302 redirection method for call forwarding. Calling-party numbers that do not match the patterns defined with this command are forwarded using Cisco-proprietary call forwarding for backward compatibility.</td>
</tr>
<tr>
<td><strong>Example:</strong> <code>call-forward pattern pattern</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> calling-number local</td>
<td>(Optional) Replaces a calling-party number and name with the forwarding-party (local) number and name.</td>
</tr>
<tr>
<td><strong>Example:</strong> <code>calling-number local</code></td>
<td></td>
</tr>
</tbody>
</table>

- **Note** When defining forwards to nonlocal numbers, it is important to note that pattern-digit matching is performed before translation-rule operations. Therefore, you should specify in this command the digits actually entered by phone users before they are translated. For more information, see the “Voice Translation Rules and Profiles” section on page 117.
<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| 6    | transfer-system (full-blind | full-consult) | Defines the call transfer method for all lines served by the router.  
**Note** For SIP networks, use only the **full-blind** keyword or the **full-consult** keyword. For more information, see the *Cisco IOS SIP Configuration Guide*.  
- **full-blind**—Calls are transferred without consultation using H.450.2 standard methods.  
- **full-consult**—Calls are transferred with consultation using H.450.2 standard methods and a second phone line if available. The calls fall back to **full-blind** if the second line is unavailable.  
**Example:**  
```
Router(config-telephony)# transfer-system full-consult
``` |
| 7    | transfer-pattern transfer-pattern | Allows transfer of telephone calls by Cisco Unified IP phones to specified phone number patterns. If no transfer pattern is set, the default is that transfers are permitted only to other local IP phones.  
**Note** When defining transfers to nonlocal numbers, it is important to note that transfer-pattern digit matching is performed before translation-rule operations. Therefore, you should specify in this command the digits that are actually entered by phone users before they are translated. For more information, see the “Voice Translation Rules and Profiles” section on page 117.  
**Example:**  
```
Router(config-telephony)# transfer-pattern 52540..
``` |
| 8    | exit | Exits telephony-service configuration mode.  
**Example:**  
```
Router(config-telephony)# exit
``` |
| 9    | dial-peer voice tag voip | Enters dial-peer configuration mode.  
**Example:**  
```
Router(config)# dial-peer voice 2 voip
``` |
| 10   | dtmf-relay rtp-nte | Forwards DTMF tones by using Real-Time Transport Protocol (RTP) with the Named Telephone Event (NTE) payload type. This enables DTMF relay using the RFC 2833 standard method.  
**Example:**  
```
Router(config-dial-peer)# dtmf-relay rtp-nte
``` |
| 11   | dtmf-relay sip-notify | Forwards DTMF tones using SIP NOTIFY messages.  
**Example:**  
```
Router(config-dial-peer)# dtmf-relay sip-notify
``` |
| 12   | exit | Exits dial-peer configuration mode.  
**Example:**  
```
Router(config-dial-peer)# exit
``` |
### Command or Action

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 13</strong> sip-ua</td>
<td>Enters SIP user-agent configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# sip-ua</td>
<td></td>
</tr>
<tr>
<td><strong>Step 14</strong> notify telephone-event max-duration time</td>
<td>Configures the maximum time interval allowed between two consecutive NOTIFY messages for a single DTMF event.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-sip-ua)# notify telephone-event max-duration 2000</td>
<td></td>
</tr>
<tr>
<td><strong>Step 15</strong> registrar (dns:host-name</td>
<td>ipv4:ip-address) expires seconds [tcp] [secondary]</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-sip-ua)# registrar ipv4:10.8.17.40 expires 3600 secondary</td>
<td></td>
</tr>
<tr>
<td><strong>Step 16</strong> retry register number</td>
<td>Sets the total number of SIP Register messages that the gateway should send.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-sip-ua)# retry register 10</td>
<td></td>
</tr>
<tr>
<td><strong>Step 17</strong> timers register time</td>
<td>Sets how long the SIP user agent (UA) waits before sending Register requests.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-sip-ua)# timers register 500</td>
<td></td>
</tr>
<tr>
<td><strong>Step 18</strong> exit</td>
<td>Exits SIP user-agent configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-sip-ua)# exit</td>
<td></td>
</tr>
</tbody>
</table>

### Verifying SIP Trunk Support Features

**Step 1** Use the `show running-config` command to verify dial-peer, telephony-service, and SIP UA parameter values.
Examples

This section contains the following examples:

- Call Forwarding over SIP Networks: Example, page 281
- Call Transfer over SIP Networks: Example, page 281
- DTMF Relay using RFC 2833: Example, page 281
- DTMF Relay using SIP Notify: Example, page 282
- SIP Register Support: Example, page 282

Call Forwarding over SIP Networks: Example
The following example enables call forwarding using the H.450.3 standard or SIP 302 response:

dial-peer voice 100 pots
destination-pattern 9.T
port 1/0/0
!
dial-peer voice 4000 voip
destination-pattern 4...
session protocol sipv2
session-target ipv4:1.1.1.1
!
telephony-service
call-forward pattern 4...

Call Transfer over SIP Networks: Example
The following example specifies transfer with consultation using the H.450.2 standard for all IP phones serviced by the router:

!
dial-peer voice 100 pots
destination-pattern 9.T
port 1/0/0
!
dial-peer voice 4000 voip
destination-pattern 4...
session protocol sipv2
session-target ipv4:1.1.1.1
!
telephony-service
transfer-pattern 4...
transfer-system full-consult

DTMF Relay using RFC 2833: Example
The following example specifies use of the RFC 2833 method for in-band DTMF relay for calls using dial peer 2.

dial-peer voice 2 voip
dtmf-relay rtp-nte

sip-ua
notify telephone-event max-duration 2000
DTMF Relay using SIP Notify: Example

The following example specifies use of the SIP notify method for in-band DTMF relay for calls using dial peer 4.

```
dial-peer voice 4 voip
dtmf-relay sip-notify
```

```
sip-ua
    notify telephone-event max-duration 2000
```

SIP Register Support: Example

The following example sets up the gateway to register the gateway’s E.164 telephone numbers with an external SIP registrar.

```
sip-ua
    registrar ipv4:10.8.17.40 expires 3600 secondary
    retry register 10
    timers register 500
```

Troubleshooting SIP Trunk Support Features

**Step 1**

The `show sip-ua status` command output displays the time interval between consecutive NOTIFY messages for a telephone event. In the following example, the time interval is 2000 ms.

```
Router# show sip-ua status
```

```
SIP User Agent Status
SIP User Agent for UDP :ENABLED
SIP User Agent for TCP :ENABLED
SIP User Agent bind status(signaling):DISABLED
SIP User Agent bind status(media):DISABLED
SIP early-media for 180 responses with SDP:ENABLED
SIP max-forwards :6
SIP DNS SRV version:2 (rfc 2782)
NAT Settings for the SIP-UA
Role in SDP:NONE
Check media source packets:DISABLED
Maximum duration for a telephone-event in NOTIFYs:2000 ms
SIP support for ISDN SUSPEND/RESUME:ENABLED
Redirection (3xx) message handling:ENABLED
SDP application configuration:
    Version line (v=) required
    Owner line (o=) required
    Timespec line (t=) required
    Media supported:audio image
    Network types supported:IN
    Address types supported:IP4
    Transport types supported:RTP/AVP udptl
```

**Step 2**

Use the `show sip-ua timers` command to show the waiting time before Register requests are sent; that is, the value that has been set with the `timers register` command.

**Step 3**

Use the `show sip-ua register status` command to show the status of local E.164 registrations.

**Step 4**

Use the `show sip-ua statistics` command to show the Register messages that have been sent.
Feature History for SIP Trunk Features

<table>
<thead>
<tr>
<th>Cisco Unified CME Version</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1</td>
<td>Support for SIP networks was introduced.</td>
</tr>
<tr>
<td>3.2</td>
<td>DTMF relay for SIP trunks was introduced.</td>
</tr>
</tbody>
</table>

Related Features

**Call Forwarding and Call Transfer on a SIP Network**
After using call forwarding commands for Cisco Unified CME, you need to configure SIP call forwarding and transfer, which are described in the “Configuring SIP Call Transfer” chapter of the *Cisco IOS SIP Configuration Guide*.

**Call Forwarding and Call Transfer for SCCP Phones**
For a more complete discussion of Cisco Unified CME call forwarding and transfer methods, see the “Transfer and Forwarding Support” section on page 223.
For information about configuring call forwarding and transfer for SCCP phones, see the “Call Forwarding” section on page 372 and the “Call Transfer” section on page 465.

**Call Forwarding and Call Transfer for SIP Phones**
For information about configuring call forwarding and transfer for SIP phones, see the *Cisco CallManager Express 3.4 Configuration Guide*.

**Prefixes for SIP Unsolicited MWI Notify Messages**
When SIP trunks are used to connect sites to a voice-mail server, a prefix can be added to extension numbers in order to distinguish the extensions at different sites. For more information, see the “MWI Prefix Specification for SIP Voice-Mail Applications” section on page 308.
Video Support for SCCP-Based Endpoints

This chapter describes how to configure SCCP-based video endpoints on Cisco Unified CallManager Express (Cisco Unified CME). It contains the following sections:

- Video Support Overview, page 285
- Configuring Video for SCCP-Based Endpoints, page 289
- Verifying Video Support for SCCP-Based Endpoints, page 295
- Examples, page 295
- Troubleshooting Video Support for SCCP-Based Endpoints, page 296
- Feature History, page 297

Note: Earlier than version 4.0, the name of this product was Cisco CallManager Express (Cisco CME). Earlier than version 3.0, the name was Cisco IOS Telephony Services (Cisco ITS).

Video Support Overview

This feature allows you to pass a video stream, with a voice call, between two video-capable SCCP endpoints and between SCCP and H.323 endpoints. Through the Cisco Unified CME router, the video-capable endpoints can communicate with each other locally, to a remote H.323 endpoint through a gateway, or through an H.323 network.

Note: For feature history, see the “Feature History” section on page 297.

Matching Endpoint Capabilities

During phone registration, information about endpoint capabilities is stored in the Cisco Unified CME. These capabilities are used to match with other endpoints during call setup. Endpoints can update at any time; however, the router recognizes endpoint-capability changes only during call setup. If a video feature is added to a phone, the information about it is updated in the router’s internal data structure, but that information does not take effect until the next call. If a video feature is removed, the router continues to see the video capability until the call is terminated but no video stream is exchanged between the two endpoints.
Video Support for SCCP-Based Endpoints

Video Support Overview

The endpoint-capability match is executed every time a new call is set up or an existing call is resumed.

Retrieving Video Codec Information

Voice gateways use dial-peer configurations to retrieve codec information for audio codecs. Video codec selection is done by the endpoints and is not controlled by the H.323 service-provider interface (SPI) through dial-peer or other configuration. The video-codec information is retrieved from the SCCP endpoint using a capabilities request during call setup.

Call Fallback to Audio-Only

When a video-capable endpoint connects to an audio-only endpoint, the call falls back to an audio-only connection. Also, for certain features, such as conferencing, where video support is not available, the call falls back to audio-only.

Cisco Unified CME routers use a call-type flag to indicate whether the call is video-capable or audio-only. The call-type flag is set to video when the video capability is matched or set to audio-only when connecting to an audio-only TDM or an audio-only SIP endpoint.

Call Setup for Video Endpoints

The process for handling SCCP video endpoints is the same as that for handling SCCP audio endpoints. The video call must be part of the audio call. If the audio call setup fails, the video call fails.

During the call setup for video, media setup handling determines if a video-media-path is required or not. If so, the corresponding video-media-path setup actions are taken.

- For an SCCP endpoint, video-media-path setup includes sending messages to the endpoints to open a multimedia path and start the multimedia transmission.
- For an H.323 endpoint, video-media-path setup includes an exchange between the endpoints to open a logical channel for the video stream.

A call-type flag is set during call setup on the basis of the endpoint-capability match. After call setup, the call-type flag is used to determine whether an additional video media path is required. Call signaling is managed by the Cisco Unified CME router, and the media stream is directly connected between the two video-enabled SCCP endpoints on the same router. Video-related commands and flow-control messages are forwarded to the other endpoint. Routers do not interpret these messages.

Call Setup Between Two Local SCCP Endpoints

For interoperability between two local SCCP endpoints (that exist on the same router), video call setup uses all existing audio-call-setup handling, except during media setup. During media setup, a message is sent to establish the video-media-path. If the endpoint responds, the video-media-path is established and a start-multimedia-transmission function is called.

Note

During an audio-only connection, all video-related media messages are skipped.
Call Setup Between SCCP and H.323 Endpoints

Call setup between SCCP and H.323 endpoints is the same as it is between SCCP endpoints except that if video capability is selected, the event is posted to the H.323 call leg to send out a video open logical channel (OLC) and the gateway generates an OLC for the video channel. Because the router needs to both terminate and originate the media stream, video must be enabled on the router before call setup begins.

Call Setup Between Two SCCP Endpoints Across an H.323 Network

If call setup between SCCP endpoints occurs across an H.323 network, the setup is a combination of the processes listed in the previous two sections. The router controls the video media setup between the two endpoints, and the event is posted to the H.323 call leg so that the gateway can generate an OLC.

Flow of the RTP Video Stream

For video streams between two local SCCP endpoints, the Real-Time Transport Protocol (RTP) stream is in flow-around mode. For video streams between SCCP and H.323 endpoints or two SCCP endpoints on different Cisco Unified CME routers, the RTP stream is in flow-through mode.

- Media flow-around mode enables RTP packets to stream directly between the endpoints of a VoIP call without the involvement of the gateway. By default, the gateway receives the incoming media, terminates the call, and then reorinates it on the outbound call leg. In flow-around mode, only signaling data is passed to the gateway, improving scalability and performance.
- With flow-through mode, the video media path is the same as for an audio call. Media packets flow through the gateway, thus hiding the networks from each other.

Use the `show voip rtp connection` command to display information about RTP named-event packets, such as caller-ID number, IP address, and port for both the local and remote endpoints, as show in the following sample output.

```
Router# show voip rtp connections
VoIP RTP active connections :
No. CallId  dstCallId  LocalRTP RmtRTP LocalIP         RemoteIP
1   102     103        18714    18158  10.1.1.1        192.168.1.1
2   105     104        17252    19088  10.1.1.1        192.168.1.1
Found 2 active RTP connections
```

Prerequisites for Configuring SCCP-Based Video Endpoints

Before you configure SCCP-based video endpoints, you must do the following:

- Establish a working H.323 or SIP network for voice calls.
- Ensure that you have a Cisco IOS image that supports this feature. Access Cisco Feature Navigator at [http://www.cisco.com/go/fn](http://www.cisco.com/go/fn).
- Ensure that the Cisco Unified CME version is 4.0 or later.
- Ensure that the Cisco Unified CallManager version is 4.0 or later.
- Ensure that the Cisco Unified IP phones are registered with the Cisco Unified CME router. Use the `show ephone registered` command to verify ephone registration.
• Ensure that the connection between the Cisco Unified Video Advantage application and the Cisco Unified IP phone is up.
  From a PC with Cisco Unified Video Advantage version 1.02 or later installed, ensure that the line between the Cisco Unified Video Advantage and the Cisco Unified IP phone is green. For more information, see the *Cisco Unified Video Advantage User Guide*.

• Ensure that the correct video firmware is installed on the Cisco Unified IP phone. Use the `show ephone phone-load` command to view current ephone firmware. The following lists the minimum firmware version for video-enabled Cisco Unified IP phones:
  - Cisco Unified IP Phone 7940G release 6.0(4)
  - Cisco Unified IP Phone 7960G release 6.0(4)
  - Cisco Unified IP Phone 7970G release 6.0(2)

  **Note** Other video-enabled endpoints, if registered with Cisco Unified CallManager, can place a video call to one of the Cisco Unified IP phones listed above, when the endpoint is registered with Cisco Unified CME.

### Restrictions for Configuring SCCP-Based Video Endpoints

Configuration restrictions for SCCP-based video endpoints are as follows:

• This feature supports only the following video codecs:
  - H.261
  - H.263

• This feature supports only the following video formats:
  - Common Intermediate Format (CIF)—Resolution 352x288
  - One-Quarter Common Intermediate Format (QCIF)—Resolution 176x144
  - Sub QIF (SQCIF)—Resolution 128x96
  - 4CIF—Resolution 704x576
  - 16CIF—Resolution 1408x1152

• The **call start fast** feature is not supported with an H.323 video connection. You must configure **call start slow** for H.323 video.

• Video capabilities are configured per ephone, not per line.

• All call feature controls (for example, mute and hold) apply to both audio and video calls, if applicable.

• This feature does not support the following:
  - Dynamic addition of video capability—The video capability must be present before the call setup starts to allow the video connection.
  - T-120 data connection between two SCCP endpoints
  - Video security
  - Far-end camera control (FECC) for SCCP endpoints
  - Video codec renegotiation—The negotiated video codec must match or the call falls back to audio-only. The negotiated codec for the existing call can be used for a new call.
Video Support for SCCP-Based Endpoints

Configuring Video for SCCP-Based Endpoints

Video codec transcoding

SIP endpoints—When a video-capable SCCP endpoint connects to a SIP endpoint, the call falls back to audio-only.

Video conferencing—The call falls back to audio-only.

Features, such as conferencing, that mix the audio streams in Cisco Unified CME—In those cases, the call falls back to audio-only.

Remote phone setup (using mtp and codec dspfarm-assist commands).

Video supplementary services between Cisco Unified CME and Cisco Unified CallManager.

- If the Cisco Unified CallManager is configured for Media Termination Point (MTP) transcoding, a video call between Cisco Unified CME and Cisco Unified CallManager is not supported.

- If an SCCP endpoint calls an SCCP endpoint on the local Cisco Unified CME and one of endpoints transferred across an H323 network, a video-consult transfer between the Cisco Unified CME systems is not supported.

- When a video-capable endpoint connects to an audio-only endpoint, the call falls back to audio-only. During audio-only calls, video messages are skipped.

- For Cisco Unified CME, the video capabilities in the vendor configuration firmware is a global configuration. This means that, although video can be enabled per ephone, the video icon shows on all Cisco Unified IP phones supported by Cisco Unified CME.

- Due to the extra CPU consumption on RTP-stream mixing, the number of video calls supported on Cisco Unified CME crossing an H.323 network is less than the maximum number of ephones supported.

- Cisco Unified CME cannot differentiate audio-only streams and audio-in-video streams. You must configure the DSCP values of audio and video streams in the H.323 dial-peers.

- If RSVP is enabled on the Cisco Unified CME, a video call is not supported.

- A separate VoIP dial peer, configured for fast-connect procedures, is required to complete a video call from a remote H.323 network to a Cisco Unity Express system.

Configuring Video for SCCP-Based Endpoints

Video capabilities are not enabled by default, and enabling video capabilities on Cisco Unified CME does not automatically enable video on all ephones. You must first enable video on Cisco Unified CME and then enable video on each ephone individually. Video parameters, like maximum bit rate, are set in video configuration mode.

You must first enable video globally for all video-capable ephones associated with a Cisco Unified CME router, and then you can set individual video parameters for each ephone.

After video is enabled globally, all video-capable ephones display the video icon.

Use the following procedures to configure SCCP-based video endpoints for Cisco Unified CME.

- Configuring Slow Connect Procedures, page 290
- Enabling Video Capabilities, page 291
- Enabling Video Capabilities for a Specific Ephone, page 292
- Resetting All Ephones, page 293
Configuring Slow Connect Procedures

Video streams require slow-connect procedures for Cisco Unified CME. H.323 endpoints also require a slow-connect because the endpoint capability match occurs after the connect message.

Note

For more information on slow-connect procedures, see Configuring Quality of Service for Voice.

Perform the following steps to configure a gateway to use slow-connect procedures.

SUMMARY STEPS

1. enable
2. configure terminal
3. voice service voip
4. h323
5. call start slow

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router&gt; enable</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router# configure terminal</td>
</tr>
<tr>
<td>Step 3 voice service voip</td>
<td>Enters voice-service configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config)# voice service voip</td>
</tr>
<tr>
<td>Step 4 h323</td>
<td>Enters H.323 voice-service configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-voi-serv)# h323</td>
</tr>
<tr>
<td>Step 5 call start slow</td>
<td>Forces an H.323 gateway to use slow-connect procedures for all VoIP calls.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-serv-h323)# call start slow</td>
</tr>
</tbody>
</table>
Enabling Video Capabilities

Use the following procedure to enable video for all video-capable phones in a CME system.

SUMMARY STEPS

1. enable
2. configure terminal
3. telephony-service
4. service phone videoCapability [0 | 1]
5. call-park system {redirect}
6. create cnf-files

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
  - Enter your password if prompted. |
| Example:          |         |
| Router> enable    |         |
| **Step 2** configure terminal | Enters global configuration mode. |
| Example:          |         |
| Router# configure terminal |         |
| **Step 3** telephony-service | Enters telephony-service configuration mode. |
| Example:          |         |
| Router(config)# telephony-service |         |
| **Step 4** service phone videoCapability [0 | 1] | Enables or disables video capabilities for Cisco Unified CME.  
  - 0—(Optional) Disables capabilities.  
  - 1—(Optional) Enables capabilities. |
| Example:          |         |
| Router(config-telephony)# service phone videoCapability 1 |         |
| **Step 5** call-park system {redirect} | Specifies system parameters for the call-park feature.  
  - redirect—Specifies that H.323 and SIP calls use H.450 or the SIP Refer method of call forwarding or transfer to park calls and to pick up calls from park. |
| Example:          |         |
| Router(config-telephony)# call-park system redirect |         |
| **Step 6** create cnf-files | Builds XML configuration files for Cisco Unified IP phones during initial system setup. The XML files created by this command are located in an in-RAM file system at system:/its. |
| Example:          |         |
| Router(config-telephony)# create cnf-files |         |
Enabling Video Capabilities for a Specific Ephone

Use the `show ephone registered` command to display the list of ephones that are registered with Cisco Unified CME. The following sample output shows that ephone 1 has video capabilities and ephone 2 is an audio-only phone.

```
Router# show ephone registered

ephone-1  Mac:0011.5C40.75E8 TCP socket:[1] activeLine:0 REGISTERED in SCCP ver 6 + Video and Server in ver 5
mediaActive:0 offhook:0 ringing:0 reset:0 reset_sent:0 paging 0 debug:0 caps:7
IP:10.1.1.6 51833 7970 keepalive 35 max_line 8
button 1: dn 1 number 8003 CH1 IDLE CH2 IDLE

ephone-2  Mac:0006.D74B.113D TCP socket:[2] activeLine:0 REGISTERED in SCCP ver 6 and Server in ver 5
mediaActive:0 offhook:0 ringing:0 reset:0 reset_sent:0 paging 0 debug:0 caps:7
IP:10.1.1.4 51123 Telecaster 7960 keepalive 36 max_line 6
button 1: dn 2 number 8004 CH1 IDLE CH2 IDLE
button 2: dn 4 number 8008 CH1 IDLE CH2 IDLE
```

Use the following procedure to enable video for an individual ephone associated with a Cisco Unified CME router.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `ephone phone-tag`
4. `video`
5. `reset`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> ephone phone-tag</td>
<td>Enters ephone configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# ephone 6</td>
<td>• <code>phone-tag</code>—Unique sequence number that identifies an ephone during configuration tasks. The maximum number is platform-dependent.</td>
</tr>
</tbody>
</table>
After video is enabled for the Cisco Unified CME system, you must reset all ephones to register the Cisco Unified CME video capability. Use the following procedure to reset all ephones.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. telephony-service
4. reset all

### Step 4

**Command or Action**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>video</td>
<td>Enables video capabilities on the specified ephone. Repeat as necessary for all ephones that require video enabled.</td>
</tr>
</tbody>
</table>

**Example:**

Router(config-ephone)# video

### Step 5

**Command or Action**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>reset</td>
<td>Performs a complete reboot of a single ephone that is associated with the Cisco Unified CME router.</td>
</tr>
</tbody>
</table>

**Note**

Alternately, you can reset all phones associated with a CME router using the reset all command in telephony-service configuration mode.

**Example:**

Router(config-ephone)# reset

### Resetting All Ephones

After video is enabled for the Cisco Unified CME system, you must reset all ephones to register the Cisco Unified CME video capability. Use the following procedure to reset all ephones.
## DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>                   .Router&gt; enable                                 </code></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>                   .Router# configure terminal                     </code></td>
</tr>
<tr>
<td><strong>Step 3</strong> telephony-service</td>
<td>Enters telephony-service configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>                   .Router(config)# telephony-service                 </code></td>
</tr>
<tr>
<td><strong>Step 4</strong> reset all</td>
<td>Resets all phones served by the Cisco Unified CME router. The router</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>pauses for 15 seconds between the reset starts for each successive</td>
</tr>
<tr>
<td></td>
<td>ephone unless the <code>time-interval</code> argument is used to change that</td>
</tr>
<tr>
<td></td>
<td>value.</td>
</tr>
<tr>
<td></td>
<td><code>                   .Router(config-telephony)# reset all               </code></td>
</tr>
</tbody>
</table>

## Setting Video Parameters

Use the following procedure to set the maximum bit rate for all video-capable phones associated with a Cisco Unified CME router.

### SUMMARY STEPS

1. enable
2. configure terminal
3. telephony-service
4. video
5. maximum bit-rate `value`
Video Support for SCCP-Based Endpoints

Verifying Video Support for SCCP-Based Endpoints

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> telephony-service</td>
<td>Enters telephony-service configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# telephony-service</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> video</td>
<td>Enters video configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-telephony)# video</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> maximum bit-rate value</td>
<td>Sets the maximum IP phone video bandwidth, in kbps. The range is 0 to 10000000. The default is 10000000.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(conf-tele-video)# maximum bit-rate 256</td>
<td></td>
</tr>
</tbody>
</table>

Verifying Video Support for SCCP-Based Endpoints

**Step 1** Use the `show running-config` command to verify the video settings in the configuration.

• Refer to the telephony-service portion of the output for commands that configure video support on the Cisco Unified CME.

• Refer to the ephone portion of the output for commands that configure video support for a specific ephone.

Examples

The following example shows the configuration for video with Cisco Unified CME:

telephony-service
  video
    maximum bit-rate 256
  load 7960-7940 P00306000404
  max-ephones 24
  max-dn 24
  ip source-address 10.0.180.130 port 2000
  service phone videoCapability 1
  timeouts interdigit 4
The following example shows the configuration for video with a specific Cisco Unified IP Phone.

```plaintext
ephone 6
video
maximum bit-rate 256
mac-address 000F.F7DE.CA5
```

### Troubleshooting Video Support for SCCP-Based Endpoints

**Step 1**
For SCCP endpoint troubleshooting, use the following `debug` commands:

- `debug cch323 video`—Enables video debugging trace on the H.323 service-provider interface (SPI).
- `debug ephone detail`—Debugs all Cisco Unified IP phones that are registered to the router, and displays error and state levels.
- `debug h225 asn1`—Displays Abstract Syntax Notation One (ASN.1) contents of H.225 messages that have been sent or received.
- `debug h245 asn1`—Displays ASN.1 contents of H.245 messages that have been sent or received.
- `debug voip ccapi inout`—Displays the execution path through the call-control application programming interface (CCAPI).

**Step 2**
For ephone troubleshooting, use the following `debug` commands:

- `debug ephone message`—Enables message tracing between Cisco Unified IP phones.
- `debug ephone register`—Sets registration debugging for Cisco Unified IP phones.
- `debug ephone video`—Sets ephone video traces, which provide information about different video states for the call, including video capabilities selection, start, and stop.

**Step 3**
For basic video-to-video call checking, use the following `show` commands:

- `show call active video`—Displays call information for SCCP video calls in progress.
- `show ephone offhook`—Displays information and packet counts for ephones that are currently off hook.
- `show ephone registered`—Displays the status of registered ephones.
- `show voip rtp connections`—Displays information about RTP named-event packets, such as caller ID number, IP address, and port for both the local and remote endpoints.
## Feature History

<table>
<thead>
<tr>
<th>Cisco Unified CME Version</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.0</td>
<td>Video support for SCCP-based endpoints was introduced.</td>
</tr>
</tbody>
</table>
Voice-Mail Support

This chapter describes features that help Cisco Unified CME interwork with various voice mail systems. It discusses the following topics:

- Cisco Unity Express Integration, page 300
- Cisco Unity Integration, page 301
- DTMF Integration for Legacy Voice-Mail Applications, page 301
- Mailbox Selection Policy for Voice-Mail Servers, page 304
- MWI Prefix Specification for SIP Voice-Mail Applications, page 308

Note

Voice-Mail Support Overview

Cisco Unified CME can be used with several different voice-mail systems to forward calls to leave messages and to receive message waiting indication (MWI).

MWI is associated with the primary extension of an IP phone, although another extensions can be selected in its place (see the “MWI Line Selection” section on page 519). MWI is indicated by a red lamp on IP phones.

For extensions associated with analog telephone adaptors (ATAs), the MWI is a lit function button on the ATA and a stutter dial tone on the connected analog phone.

Table 24 summarizes the features that are discussed in this module.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Benefit</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Unity Express Integration</td>
<td>System integrates voice-mail and auto attendant services inside Cisco routers for small and medium businesses.</td>
<td>Voice mail can be hosted on the same router as Cisco Unified CME or on another router in the network.</td>
<td>CompanyA has 30 phones and Cisco Unity Express on a single router at their location.</td>
</tr>
</tbody>
</table>
Cisco Unity Express Integration

Cisco Unity Express offers easy, one-touch access to messages and commonly used voice-mail features that enable users to reply, forward, and save messages. To improve message management, users can create alternate greetings, access envelope information, and mark or play messages based on privacy or urgency. For instructions on how to configure Cisco Unity Express, refer to the administrator guides for Cisco Unity Express.

For instructions on how to integrate Cisco Unified CME with Cisco Unity Express, refer to Integrating Cisco CallManager Express and Cisco Unity Express.

Note
Cisco Unified CME and Cisco Unity Express must both be configured before they can be integrated.
Cisco Unity Integration

Cisco Unity is a Windows 2000-based communications solution that brings you voice mail and unified messaging and integrates them with the desktop applications you use every day. Cisco Unity gives you the ability to access all of your messages—voice, fax, and e-mail—by using your desktop PC, a touchtone phone, or the Internet. The Cisco Unity voice-mail system supports voice-mail integration with Cisco Unified CME. This integration requires configuration of both the Cisco Unified CME router and Cisco Unity software to get voice-mail service.

For configuration instructions for the Cisco Unified CME router and for Cisco Unity software on a PC, refer to the *Cisco CallManager Express 3.x Integration Guide for Cisco Unity 4.0*.

DTMF Integration for Legacy Voice-Mail Applications

This feature allows you to modify DTMF patterns that provide information to legacy voice-mail systems. This section describes the following topics:

- DTMF Integration Overview, page 301
- Configuring DTMF Integration, page 302
- Verifying DTMF Integration, page 304
- Examples, page 304
- Feature History for DTMF Integration, page 304

DTMF Integration Overview

Note

For a summary of the functionality introduced in different releases, see the “Feature History for DTMF Integration” section on page 304.

For dual tone multifrequency (DTMF) integrations, information on how to route incoming or forwarded calls is sent by a telephone system in the form of DTMF digits. The DTMF digits are sent in a pattern that is based on the integration file in the voice-mail system connected to the Cisco Unified CME router. These patterns are required for the DTMF integration of Cisco Unified CME with most voice-mail systems. DTMF integration configuration on the Cisco Unified CME router works with any analog voice-mail system. Voice-mail systems are designed to respond to DTMF after the system has answered the incoming calls.

The Cisco Unified CME router provides the flexibility to integrate with any legacy voice-mail system. You can configure multiple tags and tokens for each pattern, depending on the voice-mail system and type of access. The *tag* argument used in the configuration pattern must match the number defined in the voice-mail system’s integration file to identify the type of call. The keywords—*CGN* (calling number), *CDN* (called number), and *FDN* (forwarding number)—define the type of call information that is sent to the voice-mail system.

After configuring the DTMF integration patterns on the Cisco Unified CME router, you set up the integration files on the third-party legacy voice-mail system by following the instructions in the documents that accompany the voice-mail system. You must design the DTMF integration patterns appropriately so that the voice-mail system and the Cisco Unified CME router work with each other.
Configuring DTMF Integration

This task sets up DTMF integration patterns on the Cisco Unified CME router.

**Note**
Although it is unlikely that you will use multiple instances of the CGN, CDN, or FDN keyword in a single command line, it is permissible to do so.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. vm-integration
4. pattern direct \( \text{tag1} \{ \text{CGN} | \text{CDN} | \text{FDN} \} \) \( \text{tag2} \{ \text{CGN} | \text{CDN} | \text{FDN} \} \) \( \text{tag3} \{ \text{CGN} | \text{CDN} | \text{FDN} \} \) [last-tag]
5. pattern ext-to-ext busy \( \text{tag1} \{ \text{CGN} | \text{CDN} | \text{FDN} \} \) \( \text{tag2} \{ \text{CGN} | \text{CDN} | \text{FDN} \} \) \( \text{tag3} \{ \text{CGN} | \text{CDN} | \text{FDN} \} \) [last-tag]
6. pattern ext-to-ext no-answer \( \text{tag1} \{ \text{CGN} | \text{CDN} | \text{FDN} \} \) \( \text{tag2} \{ \text{CGN} | \text{CDN} | \text{FDN} \} \) \( \text{tag3} \{ \text{CGN} | \text{CDN} | \text{FDN} \} \) [last-tag]
7. pattern trunk-to-ext busy \( \text{tag1} \{ \text{CGN} | \text{CDN} | \text{FDN} \} \) \( \text{tag2} \{ \text{CGN} | \text{CDN} | \text{FDN} \} \) \( \text{tag3} \{ \text{CGN} | \text{CDN} | \text{FDN} \} \) [last-tag]
8. pattern trunk-to-ext no-answer \( \text{tag1} \{ \text{CGN} | \text{CDN} | \text{FDN} \} \) \( \text{tag2} \{ \text{CGN} | \text{CDN} | \text{FDN} \} \) \( \text{tag3} \{ \text{CGN} | \text{CDN} | \text{FDN} \} \) [last-tag]
9. exit

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
  - Enter your password if prompted. |
| **Example:** Router> enable |
| **Step 2** configure terminal | Enters global configuration mode. |
| **Example:** Router# configure terminal |
| **Step 3** vm-integration | Enters voice-mail integration configuration mode and enables voice-mail integration with DTMF and an analog voice-mail system. |
| **Example:** Router(config) vm-integration |
Step 4  

pattern direct \( tag1 \{ \text{CGN} | \text{CDN} | \text{FDN} \} \) \( tag2 \{ \text{CGN} | \text{CDN} | \text{FDN} \} \) \( tag3 \{ \text{CGN} | \text{CDN} | \text{FDN} \} \) \( \text{last-tag} \)

**Example:**

Router(config-vm-integration) pattern direct 2 CGN *

Configures the DTMF digit pattern forwarding necessary to activate the voice-mail system when the user presses the messages button on the phone.

- The tag attribute is an alphanumeric string fewer than four DTMF digits in length. The alphanumeric string consists of a combination of four letters (A, B, C, and D), two symbols (* and #), and ten digits (0 to 9). The tag numbers match the numbers defined in the voice-mail system’s integration file, immediately preceding either the number of the calling party, the number of the called party, or a forwarding number. The Cisco SRS Telephony router supports a maximum of four tags.

- The keywords—CGN, CDN, and FDN—configure the type of call information sent to the voice-mail system, such as calling number (CGN), called number (CDN), or forwarding number (FDN).

Step 5  

pattern ext-to-ext busy \( tag1 \{ \text{CGN} | \text{CDN} | \text{FDN} \} \) \( tag2 \{ \text{CGN} | \text{CDN} | \text{FDN} \} \) \( tag3 \{ \text{CGN} | \text{CDN} | \text{FDN} \} \) \( \text{last-tag} \)

**Example:**

Router(config-vm-integration) pattern ext-to-ext busy 7 FDN * CGN *

Configures the DTMF digit pattern forwarding necessary to activate the voice-mail system once an internal extension attempts to connect to a busy extension and the call is forwarded to voice mail.

Step 6  

pattern ext-to-ext no-answer \( tag1 \{ \text{CGN} | \text{CDN} | \text{FDN} \} \) \( tag2 \{ \text{CGN} | \text{CDN} | \text{FDN} \} \) \( tag3 \{ \text{CGN} | \text{CDN} | \text{FDN} \} \) \( \text{last-tag} \)

**Example:**

Router(config-vm-integration) pattern ext-to-ext no-answer 5 FDN * CGN *

Configures the DTMF digit pattern forwarding necessary to activate the voice-mail system once an internal extension fails to connect to an extension and the call is forwarded to voice mail.

Step 7  

pattern trunk-to-ext busy \( tag1 \{ \text{CGN} | \text{CDN} | \text{FDN} \} \) \( tag2 \{ \text{CGN} | \text{CDN} | \text{FDN} \} \) \( tag3 \{ \text{CGN} | \text{CDN} | \text{FDN} \} \) \( \text{last-tag} \)

**Example:**

Router(config-vm-integration) pattern trunk-to-ext busy 6 FDN * CGN *

Configures the DTMF digit pattern forwarding necessary to activate the voice-mail system once an external trunk call reaches a busy extension and the call is forwarded to voice mail.

Step 8  

pattern trunk-to-ext no-answer \( tag1 \{ \text{CGN} | \text{CDN} | \text{FDN} \} \) \( tag2 \{ \text{CGN} | \text{CDN} | \text{FDN} \} \) \( tag3 \{ \text{CGN} | \text{CDN} | \text{FDN} \} \) \( \text{last-tag} \)

**Example:**

Router(config-vm-integration)# pattern trunk-to-ext no-answer 4 FDN * CGN *

Configures the DTMF digit pattern forwarding necessary to activate the voice-mail system when an external trunk call reaches an unanswered extension and the call is forwarded to voice mail.

Step 9  

exit

**Example:**

Router(config-vm-integration)# exit

Exits voice-mail integration configuration mode.
Verifying DTMF Integration

Step 1  Use the `show running-config` command to display the running configuration.

Examples

The following example sets up DTMF integration for a legacy voice-mail system.

```
vmlinregation
   pattern direct 2 CGN *
   pattern ext-to-ext busy 7 FDN * CGN *
   pattern ext-to-ext no-answer 5 FDN * CGN *
   pattern trunk-to-ext busy 6 FDN * CGN *
   pattern trunk-to-ext no-answer 4 FDN * CGN *
```

Feature History for DTMF Integration

<table>
<thead>
<tr>
<th>Cisco Unified CME Version</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.0</td>
<td>DTMF integration patterns were introduced.</td>
</tr>
</tbody>
</table>

Mailbox Selection Policy for Voice-Mail Servers

The mailbox selection policy allows users to specify a different voice mailbox than the default for calls before they are finally diverted to a voice-mail system. This section describes the following topics:

- Mailbox Selection Policy Overview, page 305
- Configuring Mailbox Selection Policy, page 305
- Verifying Mailbox Selection Policy, page 307
- Examples, page 307
- Feature History for Mailbox Selection Policy, page 307
- Related Features, page 308
Mailbox Selection Policy Overview

Note
For a summary of the functionality introduced in different releases, see the “Feature History for Mailbox Selection Policy” section on page 307.

Typically a voice-mail system uses the number that a caller has dialed to determine the mailbox to which a call should be sent. However, if a call has been diverted several times before reaching the voice-mail system, the mailbox that is selected might vary for different types of voice-mail systems. For example, Cisco Unity Express uses the last number to which the call was diverted before it was sent to voice mail as the mailbox number. Cisco Unity and some legacy PBX systems use the originally called number as the mailbox number.

The Mailbox Selection Policy feature allows you to provision the following options from the Cisco Unified CME configuration.

- For Cisco Unity Express, you can select the originally dialed number.
- For PBX voice-mail systems, you can select the last number to which the call was diverted before it was sent to voice mail. This option is configured on the outgoing dial peer for the voice-mail system's pilot number.
- For Cisco Unity voice mail, you can select the last number to which the call was diverted before it was sent to voice mail. This option is configured on the ephone-dn that is associated with the voice-mail pilot number.

Restrictions

The \texttt{mailbox-selection} command might not work properly in certain network topologies, including the following cases:

- When the last redirecting endpoint is not hosted on Cisco Unified CME. This may rarely occur with a PBX.
- When a call is forwarded across several SIP trunks. Multiple SIP Diversion Headers (stacking hierarchy) are not supported in Cisco IOS software.
- When a call is forwarded across non-Cisco voice gateways that do not support the optional H450.3 \texttt{originalCalledNr} field.

Configuring Mailbox Selection Policy

This procedure specifies a nondefault mailbox selection policy.

Note
For Cisco Unity Express or PBX voice-mail systems, use the \texttt{mailbox-selection} command in dial-peer configuration mode. For Cisco Unity voice mail, use the \texttt{mailbox-selection} command in ephone-dn configuration mode.

SUMMARY STEPS

1. enable
2. configure terminal
Voice-Mail Support

Mailbox Selection Policy for Voice-Mail Servers

3. `dial-peer voice tag voip`
   or
   `dial-peer voice tag pots`
4. `mailbox-selection [last-redirect-num | orig-called-num]`
5. `exit`
6. `ephone-dn dn-tag`
7. `mailbox-selection last-redirect-num`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router&gt; enable</td>
<td>* Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>
| **Step 3** `dial-peer voice tag voip`
   or
   `dial-peer voice tag pots` | Enters dial-peer configuration mode. |
| **Example:** Router(config)# dial-peer voice 7000 voip
   or
   Router(config)# dial-peer voice 35 pots | * tag—Identifies the dial peer. Valid entries are from 1 to 2147483647. |
| | **Note** This command should be used on the outbound dial peer associated with the pilot number of the voice-mail system. For systems using Cisco Unity Express, this is a VoIP dial peer. For systems using PBX-based voice mail, this is a POTS dial peer. |
| **Step 4** `mailbox-selection [last-redirect-num | orig-called-num]` | (Cisco Unity Express or PBX voice-mail systems only) Sets a policy for selecting a mailbox for calls that are diverted before being sent to a Cisco Unity Express or PBX voice-mail pilot number. |
| **Example:** Router(config-dial-peer)# mailbox-selection orig-called-num | * last-redirect-num—(PBX voice mail only) The mailbox number to which the call will be sent is the last number to divert the call (the number that sends the call to the voice-mail pilot number). |
| | * orig-called-num—(Cisco Unity Express only) The mailbox number to which the call will be sent is the number that was originally dialed before the call was diverted. |
| **Step 5** exit | Exits dial-peer configuration mode. |
| **Example:** Router(config-dial-peer)# exit | |
Voice-Mail Support

Mailbox Selection Policy for Voice-Mail Servers

Verifying Mailbox Selection Policy

Step 1
Use the `show running-config` command to display nondefault mailbox selection settings, which will be displayed in the dial-peer or the ephone-dn portion of the output.

Command or Action | Purpose
--- | ---
Step 6  | Enters ephone-dn configuration mode.
| • `dn-tag`—Identifies the ephone-dn.
| ephone-dn | Example:
| Router(config)# ephone-dn 752

Step 7  | (Cisco Unity systems only) Sets a policy for selecting a mailbox for calls that are diverted before being sent to a Cisco Unity voice-mail pilot number.
| • `last-redirect-num`—The mailbox number will be the last number to divert the call (the number that sends the call to the voice-mail pilot number).
| mailbox-selection [last-redirect-num] | Example:
| Router(config-ephone-dn)# mailbox-selection last-redirect-num

Examples

The following example sets a policy to select the mailbox of the originally called number when a call is diverted to a Cisco Unity Express or PBX voice-mail system with the pilot number 7000.

dial-peer voice 7000 voip
destination-pattern 7000
session target ipv4:10.3.34.211
codec g711ulaw
no vad
mailbox-selection orig-called-num

The following example sets a policy to select the mailbox of the last number that the call was diverted to before being diverted to a Cisco Unity voice-mail system with the pilot number 8000.

ephone-dn 825
number 8000
mailbox-selection last-redirect-num

Feature History for Mailbox Selection Policy

<table>
<thead>
<tr>
<th>Cisco Unified CME Version</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.0</td>
<td>Mailbox selection policy was introduced.</td>
</tr>
</tbody>
</table>
Related Features

Cisco Unity Express
For instructions on how to configure Cisco Unity Express, refer to the administrator guides in the Cisco Unity Express documentation.

For instructions on how to integrate Cisco Unified CME with Cisco Unity Express, refer to Integrating Cisco CallManager Express and Cisco Unity Express.

Cisco Unity
For configuration instructions for the Cisco Unified CME router and for Cisco Unity software on a PC, refer to the Cisco CallManager Express 3.x Integration Guide for Cisco Unity 4.0.

MWI Prefix Specification for SIP Voice-Mail Applications

This feature allows you to specify site codes or prefixes to distinguish among similarly numbered ranges of extensions at different sites in unsolicited SIP Notify messages for message-waiting indication (MWI). This section discusses the following topics:

- SIP MWI Prefix Specification Overview, page 308
- Configuring SIP MWI Prefix Specification, page 309
- Verifying SIP MWI Prefix Specification, page 311
- Examples, page 311
- Feature History for SIP MWI Prefix Specification, page 311
- Related Features, page 311

SIP MWI Prefix Specification Overview

Note For a summary of the functionality introduced in different releases, see the “Feature History for SIP MWI Prefix Specification” section on page 311.

Central voice-messaging servers that provide mailboxes for several Cisco Unified CME sites may use site codes or prefixes to distinguish among similarly numbered ranges of extensions at different sites. In Cisco Unified CME 4.0 and later versions, you can specify that your Cisco Unified CME system should accept unsolicited SIP Notify messages for message-waiting indication (MWI) that include a prefix string as a site identifier.

For example, an MWI message might indicate that the central mailbox number 5551234 has a voice message. In this example, the digits 555 are set as the prefix string or site identifier using the mwi prefix command. The local Cisco Unified CME system is able to convert 5551234 to 1234 and deliver the MWI to the correct phone. Without this prefix string manipulation, the system would reject an MWI indication for 5551234 as not matching the local Cisco Unified CME extension 1234.
Configuring SIP MWI Prefix Specification

This task configures the Cisco Unified CME system to accept unsolicited SIP Notify messages for MWI that include a prefix string as a site identifier.

SUMMARY STEPS

1. enable
2. configure terminal
3. sip-ua
4. mwi-server ip-address [expires seconds] [port port] [transport tcp | transport udp] [unsolicited]
5. exit
6. telephony-service
7. mwi prefix prefix-string
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> sip-ua</td>
<td>Enters SIP user-agent configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# sip-ua</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> mwi-server ip-address [expires seconds] [port port] [transport tcp</td>
<td>transport udp] [unsolicited]</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-sip-ua)# mwi-server 172.16.14.22 unsolicited</td>
<td>• ip-address—IP address of the MWI server.</td>
</tr>
<tr>
<td></td>
<td>• expires seconds—(Optional) Expiration time, in seconds. Range is from 600 to 99999. Default is 86400 (24 hours).</td>
</tr>
<tr>
<td></td>
<td>• port port-number—(Optional) Specifies the port number for the MWI server. Range is from 2000 to 9999. Default is 5060 (SIP standard port).</td>
</tr>
<tr>
<td></td>
<td>• transport tcp—(Optional) Selects TCP as the transport layer protocol. This is the default transport protocol.</td>
</tr>
<tr>
<td></td>
<td>• transport udp—(Optional) Selects UDP as the transport layer protocol. The default if these keywords are not used is TCP.</td>
</tr>
<tr>
<td></td>
<td>• unsolicited—(Optional) Sends a SIP Notify message for MWI without any need to send a Subscribe message from the Cisco Unified CME router.</td>
</tr>
<tr>
<td><strong>Step 5</strong> exit</td>
<td>Exits SIP user-agent configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-sip-ua)# exit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> telephony-service</td>
<td>Enters telephony-service configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# telephony-service</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> mwi prefix prefix-string</td>
<td>Specifies a string of digits that, if present before a known Cisco Unified CME extension number, should be recognized as a prefix.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-telephony)# mwi prefix 555</td>
<td>• prefix-string—Digit string. The maximum prefix length is 32 digits.</td>
</tr>
</tbody>
</table>
Verifying SIP MWI Prefix Specification

### Step 1
Use the `show running-config` to display the running configuration. The SIP MWI prefix settings appear in the SIP user-agent and telephony-service configuration sections of the output.

---

### Examples

The following example identifies the SIP server for MWI notification at the IP address 172.16.14.22. It states that the Cisco Unified CME system will accept unsolicited SIP Notify messages for known mailbox numbers using the prefix 555.

```
sip-ua
  mwi-server 172.16.14.22 unsolicited

telephony-service
  mwi prefix 555
```

---

### Feature History for SIP MWI Prefix Specification

<table>
<thead>
<tr>
<th>Cisco Unified CME Version</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.0</td>
<td>SIP MWI prefix specification was introduced.</td>
</tr>
</tbody>
</table>

---

### Related Features

**SIP Trunk Features**

Other features that may be needed to support SIP trunks are described in the “SIP Trunk Features” section on page 275.
Administrative and System Features

This module describes the following features that are used administratively or in a systemwide way in a Cisco Unified CME system.

- Directories, page 315
- Ephone Templates, page 318
- Ephone-dn Templates, page 322
- Feature Access Codes, page 325
- Feature Control, page 329
- Music on Hold, page 333
- Paging, page 342
- Redundant Router, page 351
- Timeouts and Tones, page 355
- XML Application Programming Interface


System Features Overview

This chapter describes features that system administrators can use to customize systemwide features or make their administration tasks easier. Table 25 summarizes those features.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Benefit</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Directories</td>
<td>System changes certain local directory parameters or adds listings to the local directory.</td>
<td>The local directory can be modified for local requirements.</td>
<td>The system administrator adds the phone numbers for headquarters offices to the local directory.</td>
</tr>
</tbody>
</table>
### Administrative and System Features Summary (Continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Benefit</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ephone Templates</td>
<td>System applies the commands in a template to one or more phones.</td>
<td>A set of commands can be applied uniformly and easily to a set of phones.</td>
<td>The system administrator creates a template for lobby phones on which certain soft keys should not appear and certain features should be blocked.</td>
</tr>
<tr>
<td>Ephone-dn Templates</td>
<td>System applies the commands in a template to one or more ephone-dns.</td>
<td>A set of commands can be applied uniformly and easily to a set of phones.</td>
<td>Secretary A takes messages for a group of 8 phones, while Secretary B takes messages for 4 others. The system administrator sets all types of call forwarding to Secretary A in one template and to Secretary B in another template.</td>
</tr>
<tr>
<td>Feature Access Codes</td>
<td>System recognizes a particular keypad sequence and invokes the requested feature.</td>
<td>Users whose phones do not have soft-key displays can access the same features by dialing special codes.</td>
<td>A maintenance technician with a wireless phone forwards his calls by dialing **1 and an extension number.</td>
</tr>
<tr>
<td>Music on Hold</td>
<td>System plays an audio file or live feed to callers on hold.</td>
<td>Callers know that they are still connected while they are on hold.</td>
<td>A customer calls a dentist’s office to check on a bill. The bookkeeper puts the customer on hold while researching the account and the customer hears music.</td>
</tr>
<tr>
<td>Paging</td>
<td>System opens a one-way audio path using phone external speakers to deliver pages.</td>
<td>Callers are able to deliver short messages to a group of phones in a single call.</td>
<td>An operator pages the phones in the jewelry department to tell them that a call is parked for their department at the park-slot with extension 2453. A clerk hears the page and uses directed call pickup to retrieve the call.</td>
</tr>
<tr>
<td>Timeouts and Tones</td>
<td>System uses timeout intervals and tones to enable call transitions in the system.</td>
<td>System administrators can adjust parameters to meet their requirements.</td>
<td>A system administrator in a busy office decreases the busy timeout to 5 seconds to allow more new calls to reach the system.</td>
</tr>
</tbody>
</table>
Directories

The Directories feature allows you to make modifications to the local directory. This section describes the following topics:

- Directories Overview, page 315
- Configuring Directories, page 315
- Verifying Directories, page 317
- Examples, page 317
- Feature History for Directories, page 318
- Related Features, page 318

Directories Overview

The local phone directory is automatically created from the entries that are made during ephone-dn configuration. Additional entries to the local Cisco Unified CME directory can be made using the directory entry command. The additional numbers can be nonlocal numbers, such as telephone numbers of other Cisco Unified CME systems used by the same corporation.

The order of the names in the directory entries can be specified; that is, whether the names appear with first names first or last names first.

The local directory that is displayed on an IP phone (item 4 in the Local Services menu) is served as an eXtensible Markup Language (XML) page that is accessed through HTTP without password protection. The no service local-directory command disables the directory HTTP service to suppress the availability of this directory.

Configuring Directories

This procedure defines the format for local directory names, adds local directory entries, or blocks the local directory display from phones.

SUMMARY STEPS

1. enable
2. configure terminal
3. telephony-service
4. directory {first-name-first | last-name-first}
5. directory entry {entry-tag number name name | clear}
6. no service local-directory
7. exit
## Administrative and System Features

### Directories

<table>
<thead>
<tr>
<th>DETAILED STEPS</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Router&gt; enable</code></td>
<td>- Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Router# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>telephony-service</code></td>
<td>Enters telephony-service configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Router(config)#</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>`directory (first-name-first</td>
<td>last-name-first)`</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>The actual directory of names and phone numbers is built using the <code>name</code> command and the <code>number</code> command in ephone-dn configuration mode.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Router(config-telephony)# directory last-name-first</code></td>
<td>When the command is set with the <code>first-name-first</code> keyword, you see the directory information displayed on the phone, for example, Jane E. Smith; and when the command is set with the <code>last-name-first</code> keyword, you see the directory information displayed on the phone as, for example, Smith, Jane E.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>`directory entry (entry-tag number name name</td>
<td>clear)`</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Router(config-telephony)# directory entry 1 5550111 name Sales</code></td>
<td>- <code>entry-tag</code>—Unique sequence number that identifies this directory entry during all configuration tasks. Range is from 1 to 100.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><code>no service local-directory</code></td>
<td>Disables local directory service on IP phones.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Router(config-telephony)# no service local-directory</code></td>
<td>- <code>number</code>—Telephone number or extension for the entry, up to 32 characters.</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td><code>exit</code></td>
<td>Exits telephony-service configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Router(config-telephony)# exit</code></td>
<td>- <code>name name</code>—Name of up to 24 characters that will appear in the directory.</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td><code>clear</code></td>
<td>Removes all directory entries.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>clear</code></td>
<td></td>
</tr>
</tbody>
</table>

---

**CiscoUnified CallManager Express System Administrator Guide**

**316**
Verifying Directories

**Step 1** Use the `show running-config` command to verify your configuration. Directory configuration commands are listed in the telephony-service portion of the output.

```
Router# show running-config
.
.
.timeout busy 10
.timeout ringing 100
caller-id name-only: enable
system message XYZ Company
web admin system name admin1 password admin1
web admin customer name Customer
edit DN through Web: enabled.
edit TIME through web: enabled.
Log (table parameters):
  max-size: 150
  retain-timer: 15
create cmf-files version-stamp Jan 01 2002 00:00:00
.transfer-system full-consult
.multicast moh 239.12.20.123 port 2000
.fxo hook-flash
.local directory service: enabled.
```

**Step 2** Use the `show telephony-service` command to display only the telephony-service configuration information.

**Step 3** Use the `show telephony-service directory-entry` command to display the entries made using the `directory entry` command.

**Examples**

The following example defines the naming order for the local directory on IP phones served by the Cisco Unified CME router:

```
telephony-service
directory last-name-first
```

The following example creates a directory of three telephone listings:

```
telephony-service
directory entry 1 14045550111 name Sales
directory entry 2 13125550122 name Marketing
directory entry 3 12135550144 name Support
```

The following example disables the local directory on IP phones served by the Cisco Unified CME router:

```
telephony-service
no service local-directory
```
Feature History for Directories

<table>
<thead>
<tr>
<th>Cisco Unified CME Version</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.0</td>
<td>The specification of name format in the local directory was introduced.</td>
</tr>
<tr>
<td>2.1</td>
<td>The ability to block the display of the local directory on phones was introduced.</td>
</tr>
<tr>
<td>3.0</td>
<td>The ability to add local directory entries in addition to those that are automatically added from ephone-dns was introduced. Authentication for local directory display was introduced.</td>
</tr>
</tbody>
</table>

Related Features

**Speed-Dial Buttons and Abbreviated Dialing Codes**

The `directory entry` command is also used to enter systemwide speed-dial definitions. For more information, see the “Speed Dial” section on page 523.

**Called-Name Display**

The `directory entry` command is also used to provide caller ID name display. For more information, see the “Called-Name Display” section on page 537.

Ephone Templates

Ephone templates allow you to combine a set of ephone commands in a template that can then be applied uniformly to one or more individual ephones. This section contains the following topics:

- Ephone Templates Overview, page 318
- Configuring Ephone Templates, page 319
- Verifying Ephone Templates, page 320
- Examples, page 321
- Feature History for Ephone Templates, page 321
- Related Features, page 321

Ephone Templates Overview

For a summary of the functionality introduced in different releases, see the “Feature History for Ephone Templates” section on page 321.

An ephone template is a set of ephone commands that can be applied to one or more individual ephones using a single command.
Ephone templates were introduced in Cisco CME 3.2 to manipulate soft-key display and order on IP phones. In Cisco Unified CME 4.0, the role of ephone templates was significantly enhanced to include a number of additional phone features. Templates allow you to uniformly and easily implement the features you select for a set of phones. A maximum of 20 ephone templates can be created in a Cisco Unified CME system, although an ephone can have only one template applied to it at a time.

If you use an ephone template to apply a command to a phone and you also use the same command in ephone configuration mode for the same phone, the value that you set in ephone configuration mode has priority.

**Note**
The features that can be implemented using ephone templates are available in CLI help. Use the following syntax to list the available commands:

```
Router(config)# ephone-template
Router(config-ephone-template)# ?
```

## Configuring Ephone Templates

This procedure creates an ephone template and applies it to an ephone.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `ephone-template template-tag`
4. `command`
5. `exit`
6. `ephone phone-tag`
7. `ephone-template template-tag`
8. `restart`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>
### Command or Action

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 3 | **ephone-template template-tag** | Enters ephone-template configuration mode to create an ephone template.  
- **template-tag**—Unique identifier for the ephone template that is being created. Range is from 1 to 20. |
| Example: | `Router(config)# ephone-template 15` |  |
| Step 4 | **command** | Applies the specified command to the ephone template that is being created. See CLI help for a list of commands that can be used in this step. Repeat this step for each command that you want to add to the ephone template. |
| Example: | `Router(config-ephone-template)# features blocked Park Transfer` |  |
| Step 5 | **exit** | Exits ephone-template configuration mode. |
| Example: | `Router(config-ephone-template)# exit` |  |
| Step 6 | **ephone phone-tag** | Enters ephone configuration mode.  
- **phone-tag**—Unique sequence number that identifies this ephone during configuration tasks. |
| Example: | `Router(config)# ephone 36` |  |
| Step 7 | **ephone-template template-tag** | Applies an ephone template to the ephone that is being configured. |
| Example: | `Router(config-ephone)# ephone-template 15` |  |
| Step 8 | **restart** | Performs a fast reboot of this ephone. Does not contact the DHCP or TFTP server for updated information.  
**Note** You can restart all ephones using the **restart all** command in telephony-service configuration mode. |
| Example: | `Router(config-ephone)# restart` |  |

### Verifying Ephone Templates

**Step 1** Use the **show running-config** command to display the running configuration. Ephones with templates applied to them are listed in the ephone portion of the output. Ephone template information is listed in the ephone-template part of the output.

**Step 2** Use the **show telephony-service ephone** and **show telephony-service ephone-template** commands to display only the ephone template information.
Examples

The following example creates an ephone template to block the use of Park and Transfer soft keys. It is applied to ephone 36 and extension 2333.

```plaintext
ephone-template 15
   features blocked Park Transfer

ephone-dn 2
   number 2333

ephone 36
   button 1:2
   ephone-template 15
```

Feature History for Ephone Templates

<table>
<thead>
<tr>
<th>Cisco Unified CME Version</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.2</td>
<td>Ephone templates were introduced to manage soft keys. The only commands that can be used in ephone templates are the <strong>softkeys</strong> commands.</td>
</tr>
</tbody>
</table>
| 4.0                       | • The number of ephone templates that can be created was increased from 5 to 20.  
                            • More commands can be included in ephone templates. |

Related Features

**Ephone-dn Templates**

Ephone-dn templates allow you to create a set of ephone-dn commands and apply them to one or more individual ephone-dns. For more information, see the “Ephone-dn Templates” section on page 322.

**Soft-Key Display**

The display of soft keys during different call states is managed using ephone templates. For more information, see the “Soft-Key Display” section on page 551.
Ephone-dn Templates

Ephone-dn templates are a set of ephone-dn commands that can be applied together to one or more ephone-dns. This section contains the following topics:

- Ephone-dn Templates Overview, page 322
- Configuring Ephone-dn Templates, page 322
- Verifying Ephone-dn Templates, page 323
- Examples, page 324
- Feature History for Ephone-dn Templates, page 324
- Related Features, page 324

Ephone-dn Templates Overview

Note
For a summary of the functionality introduced in different releases, see the “Feature History for Ephone-dn Templates” section on page 324.

Ephone-dn templates allow you to apply a standard set of features to ephone-dns. A maximum of 15 ephone-dn templates can be created in a Cisco Unified CME system, although an ephone-dn can have only one template applied to it at a time.

If you use an ephone-dn template to apply a command to an ephone-dn and you also use the same command in ephone-dn configuration mode for the same ephone-dn, the value that you set in ephone-dn configuration mode has priority.

Note
The features that can be implemented using ephone-dn templates are available in CLI help. Use the following syntax to list the available commands:

```
Router(config)# ephone-dn-template 1
Router(config-ephone-dn-template)# ?
```

Configuring Ephone-dn Templates

This procedure creates an ephone-dn template and applies it to an ephone-dn.

SUMMARY STEPS

1. enable
2. configure terminal
3. ephone-dn-template template-tag
4. command
5. exit
6. ephone-dn dn-tag
7. ephone-dn-template template-tag
**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td>Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> ephone-dn-template template-tag</td>
<td>Enters ephone-dn-template configuration mode to create an ephone-dn template.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# ephone-dn-template 3</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> command</td>
<td>Applies the specified command to the ephone-dn template that is being created. See CLI help for a list of commands that can be used in this step. Repeat this step to add more commands to the template.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-ephone-dn-template)# call-forwarding busy 4000</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> exit</td>
<td>Exits ephone-dn-template configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-ephone-dn-template)# exit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> ephone-dn dn-tag</td>
<td>Enters ephone-dn configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# ephone-dn 23</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> ephone-dn-template template-tag</td>
<td>Applies an ephone-dn template to the ephone-dn that is being configured.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-ephone-dn)# ephone-dn-template 3</td>
<td></td>
</tr>
</tbody>
</table>

**Verifying Ephone-dn Templates**

**Step 1** Use the show running-config command to display the running configuration. Ephone-dns with templates applied to them are listed in the ephone-dn portion of the output. Ephone-dn template information is listed in the ephone-dn-template part of the output.

**Example:**

Router# show running-config

ephone-dn-template 1
description Call Center Line 1
call-forward busy 500
call-forward noan 500 timeout 10
pickup-group 33!
!
Step 2  Use the `show telephony-service ephone-dn` and `show telephony-service ephone-dn-template` commands to display only the ephone-dn template information.

Examples

The following example creates ephone-dn template 3, which sets call forwarding on busy and no answer to forward calls to extension 4000 and sets the pickup group to 4. Ephone-dn template 3 is then applied to ephone-dn 23 and ephone-dn 33, which appear on ephones 13 and 14, respectively.

```
ephone-dn-template 3
  call-forwarding busy 4000
  call-forwarding noan 4000 timeout 30
  pickup group 4

ephone-dn 23
  number 2323
  ephone-dn-template 3

ephone-dn 33
  number 3333
  ephone-dn-template 3

ephone 13
  button 1:23

ephone 14
  button 1:33
```

Feature History for Ephone-dn Templates

<table>
<thead>
<tr>
<th>Cisco Unified CME Version</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.0</td>
<td>Ephone-dn templates were introduced.</td>
</tr>
</tbody>
</table>

Related Features

**Ephone Templates**

Ephone templates allow you to create a set of ephone commands and apply them to one or more individual ephones. For more information, see the “Ephone Templates” section on page 318.
Feature Access Codes

Feature Access Codes (FACs) are special patterns of keypad characters that are dialed to engage particular features. This section contains the following topics:

- Feature Access Codes Overview, page 325
- Configuring Feature Access Codes, page 326
- Verifying Feature Access Codes, page 328
- Examples, page 328
- Feature History for Feature Access Codes, page 329

Feature Access Codes Overview

Note

For a summary of the functionality introduced in different releases, see the “Feature History for Feature Access Codes” section on page 329.

Feature access codes (FACs) are short sequences of digits that are dialed from a telephone keypad to invoke particular features. FACs are generally used on analog phones, while IP phones use soft keys to invoke the same features. FACs may be followed by additional digits. For example to pick up a call in pickup group 24 using the standard FAC, you would dial **4 24.

In Cisco Unified CME 4.0 and later versions, the same FACs that are used on analog phones can be enabled on IP phones. This allows phone users to access features in the same manner no matter what phone they use. FACs are disabled on IP phones until they are explicitly enabled using the fac standard command. The fac command can be used to enable the standard set of FACs shown in Table 26 or it can be used to define custom FACs or aliases.

All FACs except the call-park FAC are valid only immediately after a phone is taken off hook. The call-park FAC is considered a transfer to a call-park slot and therefore is only valid after the Transfer soft key (IP phones) or hookflash (analog phones) has been used to initiate a transfer.

<table>
<thead>
<tr>
<th>Standard FAC</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>**1 plus optional extension number</td>
<td>Call forward all.</td>
</tr>
<tr>
<td>**2</td>
<td>Call forward all cancel.</td>
</tr>
<tr>
<td>**3</td>
<td>Pick up local group.</td>
</tr>
<tr>
<td>**4 plus group number</td>
<td>Pick up different group.</td>
</tr>
<tr>
<td>**5 plus extension number</td>
<td>Pick up direct extension.</td>
</tr>
<tr>
<td>**6 plus optional park-slot number</td>
<td>Call park.</td>
</tr>
<tr>
<td>**7</td>
<td>Do not disturb.</td>
</tr>
<tr>
<td>**8</td>
<td>Redial.</td>
</tr>
<tr>
<td>**9</td>
<td>Dial voice-mail number.</td>
</tr>
<tr>
<td>*3 plus optional hunt group number</td>
<td>Join ephone-hunt group.</td>
</tr>
</tbody>
</table>

Table 26 Standard FACs
Configuring Feature Access Codes

This procedure enables standard FACs or creates custom FACs.

SUMMARY STEPS

1. enable
2. configure terminal
3. telephony-service
4. fac standard | custom \{fac-type new-code | alias tag new-code to old-code\}

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1  enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td>Step 2  configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3  telephony-service</td>
<td>Enters telephony-service configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# telephony-service</td>
<td></td>
</tr>
</tbody>
</table>
**Feature Access Codes**

### Command or Action

| Step 4 | **fac** standard | custom *(fac-type new-code | alias tag new-code to old-code)* |

Example:

Router(config-telephony)# fac custom callfwd *#5

### Purpose

Enables standard FACs or creates a custom FAC or alias.

- **standard**—Enable standard FACs for all phones.
- **custom**—Create a custom FAC for a FAC type.
- **fac-type**—Type of FAC. Choose one of the following:
  - **callfwd all**—Call forward all calls. Standard FAC is **1.** You may dial a forwarding destination number after the FAC.
  - **callfwd cancel**—Cancel call forward all calls. Standard FAC is **2.**
  - **dnd**—Do not disturb. Standard FAC is **7.**
  - **ephone-hunt join**—Join an ephone-hunt group. You must dial the tag number of the hunt group after the FAC if there is more than one hunt group that accepts dynamic login. Standard FAC is *3.
  - **ephone-hunt cancel**—Leave an ephone-hunt group. Standard FAC is #3.
  - **ephone-hunt hlog**—Hlog at the ephone-dn level (display phones only). Standard FAC is *4.
  - **ephone-hunt hlog-phone**—Hlog at the ephone level (display phones only). Standard FAC is *5.
  - **park**—Park a call. Standard FAC is **6.
  - **pickup direct**—Pick up calls from any extension. Standard FAC is **5.** You must dial the extension number after the FAC.
  - **pickup group**—Pick up calls from a non-local group. Standard FAC is **4.** You must dial the group number after the FAC.
  - **pickup local**—Pick up calls in the local group. Standard FAC is **3.
  - **redial**—Redial the last number called. Standard FAC is **8.
  - **voicemail**—Dial the voice-mail number. Standard FAC is **9.

- **new-code**—New FAC for the specified feature or alias.
- **alias**—Create a custom FAC for a predefined FAC or a predefined FAC plus extra digits.
- **tag**—Unique identifying number for this alias.
- **old-code**—Existing FAC for which you are creating an alias. This can contain numbers in addition to the FAC.

### Note

Repeat this command to set more than one custom FAC code or alias.
Verifying Feature Access Codes

**Step 1** Use the **show running-config** command to display the running configuration. FACs are listed in the telephony-service part of the output.

```plaintext
Router# show running-config
telephony-service
 fxo hook-flash
 load 7960-7940 P00307020300
 load 7914 S00104000100
 max-ephones 100
 max-dn 500
 ip source-address 10.123.23.231 port 2000
 max-redirect 20
 timeouts ringing 100
 system message XYZ Company
 voicemail 7189
 max-conferences 8 gain -6
 call-forward pattern .T
 moh flash:music-on-hold.au
 multicast moh 239.15.10.1 port 2000
 web admin system name admin1 password admin1
 dn-webedit
 time-webedit
 transfer-system full-consult
 secondary-dialtone 9
 fac custom callfwd all **1
 fac custom callfwd cancel **2
 fac custom pickup local **3
 fac custom pickup group *7
 fac custom pickup direct **5
 fac custom park *8
 fac custom dnd **7
 fac custom redial #8
 fac custom voicemail **9
 fac custom ephone-hunt join *3
 fac custom ephone-hunt cancel #3
 create cnf-files version-stamp Jan 01 2002 00:00:00
```

**Step 2** Use the **show telephony-service** command to display only the telephony-service configuration information.

**Examples**

The following example enables standard FACs for all IP phones:

```plaintext
telephony-service
 fac standard
```

The following example changes the standard call-forward-all FAC to a custom FAC:

```plaintext
telephony-service
 fac custom callfwd all *45
```
The following example creates an alias with an identifier (tag) of 5 for the group pickup of group 123. The alias substitutes the digits #4 for the standard FAC for group pickup (**4) and the group number (123). After this code is configured in the system, a phone user can simply dial #4 to pick up a ringing call in group 123 (instead of **4123).

telephony-service
fac custom alias 5 #4 to **4123

Feature History for Feature Access Codes

<table>
<thead>
<tr>
<th>Cisco Unified CME Version</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.0</td>
<td>Feature access codes were introduced.</td>
</tr>
</tbody>
</table>

Feature Control

Feature control allows you to block one or more features from specified phones. This section includes the following topics:

- Feature Control Overview, page 329
- Configuring Feature Control, page 330
- Verifying Feature Control, page 331
- Examples, page 332
- Feature History for Feature Control, page 332
- Related Features, page 332

Feature Control Overview

Note

For a summary of the functionality introduced in different releases, see the “Feature History for Feature Control” section on page 332.

In Cisco Unified CME 4.0 and later versions, individual soft-key features can be blocked for one or more phones. You specify the features that you want blocked by adding the features blocked command to an ephone template. The template is then applied under ephone configuration mode to one or more phones. If a feature is blocked using the features blocked command, the soft key is not removed, but it does not function. To remove a soft-key display, use the appropriate no softkeys command.
Configuring Feature Control

This procedure blocks one or more features for individual ephones.

SUMMARY STEPS

1. enable
2. configure terminal
3. ephone-template template-tag
4. features blocked [CFwdAll] [Confrn] [GpickUp] [Park] [PickUp] [Trnsfer]
5. exit
6. ephone phone-tag
7. ephone-template template-tag
8. restart
9. Repeat Step 6 through Step 8 for each phone to which the template should be applied.

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3 ephone-template template-tag</td>
<td>Enters ephone-template configuration mode.</td>
</tr>
<tr>
<td>Example: Router(config)# ephone-template 1</td>
<td></td>
</tr>
<tr>
<td>Step 4 features blocked [CFwdAll] [Confrn] [GpickUp] [Park] [PickUp] [Trnsfer]</td>
<td>Prevents the specified soft key from invoking its feature.</td>
</tr>
<tr>
<td>Example: Router(config-ephone-template)# features blocked Park Trnsfer</td>
<td></td>
</tr>
</tbody>
</table>
### Verifying Feature Control

**Step 1** Use the `show running-config` command to display the running configuration, including ephone templates and ephone configurations.

**Step 2** Use the `show telephony-service ephone-template` command and the `show telephony-service ephone` command to display only the contents of ephone templates and the ephone configurations.
Examples

The following example blocks the use of Park and Transfer soft keys on extension 2333.

```plaintext
ephone-template 1
  features blocked Park Trnsfer

ephone-dn 2
  number 2333

ephone 3
  button 1:2
  ephone-template 1
```

The following example blocks the use of the conference feature on extension 2579, which is on an analog phone.

```plaintext
ephone-template 1
  features blocked Confrn

ephone-dn 78
  number 2579

ephone 3
  ephone-template 1
  mac-address C910.8E47.1282
  type anl
  button 1:78
```

Feature History for Feature Control

<table>
<thead>
<tr>
<th>Cisco Unified CME Version</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.0</td>
<td>Feature control was introduced.</td>
</tr>
</tbody>
</table>

Related Features

Ephone Templates

Feature Control is applied to individual ephones using ephone templates. For more information, see the “Ephone Templates” section on page 318.

Soft-Key Display

When you use Feature Control to block a feature, the soft key for that feature remains displayed but it does not function. To remove the display of a soft key, use the appropriate `softkeys` command. For more information, see the “Soft-Key Display” section on page 551.
Music on Hold

Music on hold (MOH) is an audio stream that is played to PSTN and VoIP G.711 or G.729 callers who are placed on hold by phones in a Cisco Unified CME system. This section contains the following topics:

- Music on Hold Overview, page 333
- Configuring Music on Hold, page 334
- Verifying Music on Hold, page 341
- Examples, page 341
- Feature History for Music on Hold, page 342

Music on Hold Overview

For a summary of the functionality introduced in different releases, see the “Feature History for Music on Hold” section on page 342.

Music on hold (MOH) is an audio stream that is played to PSTN and VoIP G.711 or G.729 callers who are placed on hold by phones in a Cisco Unified CME system. This audio stream is intended to reassure callers that they are still connected to their calls. MOH is not played to local Cisco Unified CME phones that are on hold with other Cisco Unified CME phones; these parties hear a periodic repeating tone instead.

The audio stream that is used for MOH can derive from one of two sources: an audio file or a live feed. If both are configured concurrently on the Cisco Unified CME router, the router seeks the live feed first. If the live feed is found, it displaces the audio file source. If the live feed is not found or fails at any time, the router falls back to the audio file source that was specified for MOH during configuration.

If the MOH audio stream is also identified as a multicast source, the Cisco Unified CME router additionally transmits the stream on the physical IP interfaces of the Cisco Unified CME router that you specify during configuration, which permits external devices to have access to it.

A MOH audio stream from an audio file is supplied from an .au or .wav file held in router flash memory. A MOH audio stream from a live feed is supplied from a standard line-level audio connection that is directly connected to the router through an FXO or “ear and mouth” (E&M) analog voice port. The live-feed feature is typically used to connect to a CD jukebox player. Only one live MOH feed is supported per system.

When the phone receiving MOH is part of a system that uses a G.729 codec, transcoding is required between G.711 and G.729. The G.711 MOH must be translated to G.729. Note that because of compression, MOH using G.729 is of significantly lower fidelity than MOH using G.711. For information about transcoding, refer to the “Transcoding Support” section on page 199 of this guide.

In Cisco Unified CME 4.0 and later versions, internal calls are able to hear MOH, but the multicast moh command must be used to enable the flow of packets to the subnet on which the phones are located. Internal extensions that are connected through an analog voice gateway (Cisco VG 224) or through a WAN (remote extensions) do not hear MOH on internal calls.

Certain IP phones do not support IP multicast and, therefore, do not support multicast MOH. To disable multicast MOH to individual phones that do not support multicast, use the no multicast-moh command in ephone or ephone-template configuration mode.
Configuring Music on Hold

This section explains how to configure music on hold from an audio file or a live feed. It contains the following sections:

- Configuring Music on Hold from an Audio File, page 334
- Configuring Music on Hold from a Live Feed, page 337

Configuring Music on Hold from an Audio File

This section explains how to configure music on hold when you are using a file to supply the audio stream. You can also optionally specify that this audio stream should be multicast on router interfaces.

If MOH from an audio file and MOH from a live feed are both configured on the Cisco Unified CME router, the router seeks the live feed first. If a live feed is found, it displaces an audio file source. If the live feed is not found or fails at any time, the router falls back to the audio file source.

To change the audio file to a different file, you must remove the first file using the \texttt{no moh} command before specifying a second file, as shown in the following example:

\begin{verbatim}
Router(config-telephony)# no moh file1
Router(config-telephony)# moh file2
\end{verbatim}

If you configure a second file without removing the first file, the MOH mechanism stops working and may require a router reboot to clear the problem.

\textbf{Note}

If the phones receiving MOH are part of a system that uses G.729, transcoding is required between G.711 and G.729. For information about transcoding, see the “Transcoding Support” section on page 199.

You can use the \texttt{no multicast-moh} command to disable MOH for individual phones that do not support IP multicast.

Prerequisites

A music file must be in stored in the router’s flash memory. This file should be in G.711 format. The file can be in .au or .wav file format, but the file format must contain 8-bit 8-kHz data; for example, ITU-T A-law or mu-law data format.

Restrictions

- IP phones do not support multicast at 224.x.x.x addresses.
- The volume level of a MOH file cannot be adjusted through the Cisco IOS software, so it cannot be changed once the file is loaded into the flash memory of the router. To adjust the volume level of a MOH file, edit the file in an audio editor prior to downloading the file to router flash memory.

**SUMMARY STEPS**

1. \texttt{enable}
2. \texttt{configure terminal}
3. \texttt{telephony-service}
4. \texttt{moh filename}
5. `multicast moh ip-address port port-number [route ip-address-list]`

6. `exit`

7. `ephone phone-tag`

8. `multicast-moh`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> telephony-service</td>
<td>Enters telephony-service configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# telephony-service</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> moh filename</td>
<td>Configures music on hold using the specified file.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>• <code>filename</code>—Source of the audio stream for MOH.</td>
</tr>
<tr>
<td>Router(config-telephony)# moh minuet.au</td>
<td>Note If you specify a filename with this command and later want to use a different file, you must disable use of the first file with the <code>no moh</code> command before configuring the second file.</td>
</tr>
</tbody>
</table>
### Music on Hold

**Administrative and System Features**

**Step 5**

```
multicast moh ip-address port port-number [route ip-address-list]
```

**Example:**

```
Router(config-telephony)# multicast moh 239.10.16.4
port 2123 route 10.10.29.17 10.10.29.33
```

(Optional, but required for MOH on internal calls)

Specifies that the MOH audio stream should also be multicast as specified.

- **ip-address**—Specifies that this audio stream is to be used for multicast as well as for MOH, and specifies the destination IP address for multicast.
- **port port-number**—Media port for multicast. Range is from 2000 to 65535. Port 2000 is recommended because it is already used for normal RTP media transmissions between IP phones and the router.
- **route**—(Optional) Specifies a list of explicit router interfaces for the IP multicast packets.
- **ip-address-list**—(Optional) List of up to four explicit routes for multicast MOH. The default is that the MOH multicast stream is automatically output on the interfaces that correspond to the address that was configured with the `ip source-address` command.

**Note**

For MOH on internal calls, packet flow must be enabled to the subnet on which the phones are located.

---

**Step 6**

```
exit
```

**Example:**

```
Router(config-telephony)# exit
```

Exits telephony-service configuration mode.

---

**Step 7**

```
ephone phone-tag
```

**Example:**

```
Router(config)# ephone 28
```

Enters ephone configuration mode.

---

**Step 8**

```
multicast-moh
```

**Example:**

```
Router(config-ephone)# no multicast-moh
```

(Optional) Enables multicast MOH on a phone. This is the default.

The `no` form of the command disables MOH for phones that do not support multicast. Callers hear a repeating tone when they are placed on hold.

**Note**

This command can also be made part of an ephone template that is applied to one or more phones.
Configuring Music on Hold from a Live Feed

To configure MOH from a live feed, you establish a voice port and dial peer for the call and also create a “dummy” ephone-dn. The ephone-dn must have a phone or extension number assigned to it so that it can make and receive calls, but the number is never assigned to a physical phone.

The recommended interface for live-feed MOH is an analog E&M port because it requires the minimum number of external components. You connect a line-level audio feed (standard audio jack) directly to pins 3 and 6 of an E&M RJ-45 connector. The E&M voice interface card (VIC) has a built-in audio transformer that provides appropriate electrical isolation for the external audio source. (An audio connection on an E&M port does not require loop-current). The signal immediate and auto-cut-through commands disable E&M signaling on this voice port. A G.711 audio packet stream is generated by a digital signal processor (DSP) on the E&M port.

If you are using an FXO voice port for live-feed MOH instead of an E&M port, connect the MOH source to the FXO voice port. This connection requires an external adapter to supply normal telephone company (telco) battery voltage with the correct polarity to the tip and ring leads of the FXO port. The adapter must also provide transformer-based isolation between the external audio source and the tip and ring leads of the FXO port.

Music from a live feed is continuously fed into the MOH playout buffer instead of being read from a flash file, so there is typically a 2-second delay. An outbound call to a MOH live-feed source is attempted (or reattempted) every 30 seconds until the connection is made by the directory number that has been configured for MOH. If the live-feed source is shut down for any reason, the flash memory source will be automatically activated.

A live-feed MOH connection is established as an automatically connected voice call that is made by the Cisco Unified CME MOH system itself or by an external source directly calling in to the live-feed MOH port. An MOH call can be from or to the PSTN or can proceed via VoIP with voice activity detection (VAD) disabled. The call is assumed to be an incoming call unless the optional out-call keyword is used with the moh command during configuration.

The Cisco Unified CME router uses the audio stream from the call as the source for the MOH stream, displacing any audio stream that is available from a flash file. An example of an MOH stream received over an incoming call is an external H.323-based server device that calls the ephone-dn to deliver an audio stream to the Cisco Unified CME router.

Note

If the phones receiving MOH are part of a system that uses G.729, transcoding is required between G.711 and G.729. For information about transcoding, refer to the “Transcoding Support” section on page 199 of this guide.

You can use the no multicast-moh command to disable MOH for individual phones that do not support IP multicast.

Restrictions

- An FXO port can be used for a live feed if the port is supplied with an external third-party adapter to provide a battery feed.
- An foreign exchange station (FXS) port cannot be used for a live feed.
- For a live feed from VoIP, VAD must be disabled.
## SUMMARY STEPS

1. enable
2. configure terminal
3. voice-port `port`
4. input gain `decibels`
5. auto-cut-through (E&M only)
6. operation 4-wire (E&M only)
7. signal immediate (E&M only)
8. exit
9. dial peer voice tag pots
10. destination-pattern `string`
11. port `port`
12. exit
13. ephone-dn `dn-tag`
14. number `number`
15. moh [out-call `outcall-number`] [ip `ip-address` port `port-number` [route `ip-address-list`]]
16. exit
17. ephone `phone-tag`
18. multicast-moh

## DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> voice-port <code>port</code></td>
<td>Enters voice-port configuration mode. To find the correct definition of</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>the <code>port</code> argument for your router, refer to the <code>Cisco IOS Voice Command Reference</code>.</td>
</tr>
<tr>
<td>Router(config)# voice-port 1/1/0</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> input gain <code>decibels</code></td>
<td>Specifies, in decibels, the amount of gain to be inserted at the</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>receiver side of the interface. Acceptable values are integers from –6</td>
</tr>
<tr>
<td>Router(config-voice-port)# input gain</td>
<td>to 14.</td>
</tr>
<tr>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><strong>auto-cut-through</strong>&lt;br&gt;(E&amp;M ports only) Enables call completion when a PBX does not provide an M-lead response. MOH requires that you use this command with E&amp;M ports.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-voice-port)# auto-cut-through</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>operation 4-wire&lt;br&gt;(E&amp;M ports only) Selects the 4-wire cabling scheme. MOH requires that you specify 4-wire operation with this command for E&amp;M ports.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-voice-port)# operation 4-wire</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>signal immediate&lt;br&gt;(E&amp;M ports only) For E&amp;M tie trunk interfaces, directs the calling side to seize a line by going off-hook on its E-lead and to send address information as dual tone multifrequency (DTMF) digits.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-voice-port)# signal immediate</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>exit&lt;br&gt;Exits voice-port configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-voice-port)# exit</td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td>dial peer voice tag pots&lt;br&gt;Enters dial-peer configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config)# dial peer voice 7777 pots</td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td>destination-pattern string&lt;br&gt;Specifies either the prefix or the full E.164 telephone number to be used for a dial peer.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-dial-peer)# destination-pattern 7777</td>
</tr>
<tr>
<td><strong>Step 11</strong></td>
<td>port port&lt;br&gt;Associates the dial peer with the voice port that was specified in <strong>Step 3</strong>.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-dial-peer)# port 1/1/0</td>
</tr>
<tr>
<td><strong>Step 12</strong></td>
<td>exit&lt;br&gt;Exits dial-peer configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-dial-peer)# exit</td>
</tr>
<tr>
<td><strong>Step 13</strong></td>
<td>ephone-dn dn-tag&lt;br&gt;Enters ephone-dn configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config)# ephone-dn 55</td>
</tr>
<tr>
<td><strong>Step 14</strong></td>
<td>number number&lt;br&gt;Configures a valid extension number for this ephone-dn instance. This number is not assigned to any phone; it is only used to make and receive calls that contain an audio stream to be used for MOH.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-ephone-dn)# number 5555</td>
</tr>
</tbody>
</table>
## Music on Hold

### Command or Action

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>15</td>
<td>moh [out-call outcall-number] [ip ip-address port port-number [route ip-address-list]]</td>
<td>Specifies that this ephone-dn is to be used for an incoming or outgoing call that is to be the source for an MOH stream. If this command is used without the out-call keyword, the MOH stream is received from an incoming call.</td>
</tr>
<tr>
<td></td>
<td>Example: Router(config-ephone-dn)# moh out-call 7777 ip 239.10.16.8 port 2311 route 10.10.29.3 10.10.29.45</td>
<td></td>
</tr>
</tbody>
</table>

- **out-call outcall-number**—(Optional) Indicates that the router is calling out for a live feed that is to be used for MOH and specifies the number to be called. Forces a connection to the local router voice port that was specified in Step 3.

- **ip ip-address**—(Optional) Indicates that this audio stream is to be used as a multicast source as well as for MOH, and specifies the destination IP address for multicast.

  Note: If you specify a multicast address with this command and a different multicast address with the multicast moh command under telephony-service configuration mode, you can send the MOH audio stream to two multicast addresses.

- **port port-number**—(Optional) Media port for multicast. Range is from 2000 to 65535. Port 2000 is recommended because it is already used for RTP media transmissions between IP phones and the router.

- **route ip-address-list**—(Optional) Indicates specific router interfaces on which to transmit the IP multicast packets. Up to four IP addresses can be listed. The default is that the MOH multicast stream is automatically output on the interfaces that correspond to the address that was configured with the ip source-address command.

<table>
<thead>
<tr>
<th>Step</th>
<th>exit</th>
<th>Exits ephone-dn configuration mode.</th>
</tr>
</thead>
<tbody>
<tr>
<td>16</td>
<td></td>
<td>Example: Router(config-ephone-dn)# exit</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step</th>
<th>ephone phone-tag</th>
<th>Enters ephone configuration mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>17</td>
<td>Router(config)# ephone 28</td>
<td>(Optional) Enables multicast MOH on a phone. This is the default. The no form of the command disables MOH for phones that do not support multicast. Callers hear a repeating tone when they are placed on hold.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step</th>
<th>multicast-moh</th>
<th>This command can also be made part of an ephone template that is applied to one or more phones.</th>
</tr>
</thead>
<tbody>
<tr>
<td>18</td>
<td>Router(config-ephone)# no multicast-moh</td>
<td></td>
</tr>
</tbody>
</table>
Verifying Music on Hold

**Step 1** Use the **show running-config** command to display the running configuration. MOH commands are listed in the telephony-service part of the output.

```
Router# show running-config

telephony-service
  fxo hook-flash
  load 7960-7940 P00307020300
  load 7914 S00104000100
  max-ephones 100
  max-dn 500
  ip source-address 10.123.23.231 port 2000
  max-redirect 20
  timeouts ringing 100
  system message XYZ Company
  voicemail 7189
  max-conferences 8 gain -6
  call-forward pattern .T
  moh flash:music-on-hold.au
  multicast moh 239.15.10.1 port 2000
  web admin system name admin1 password admin1
  dn-webedit
  time-webedit
  transfer-system full-consult
  secondary-dialtone 9
  fac custom callfwd all **1
  fac custom callfwd cancel **2
  fac custom pickup local **3
  fac custom pickup group *7
  fac custom pickup direct **5
  fac custom park *8
  fac custom dnd **7
  fac custom redial #8
  fac custom voicemail **9
  fac custom ephone-hunt join *3
  fac custom ephone-hunt cancel #3
create cnf-files version-stamp Jan 01 2002 00:00:00
```

**Step 2** Use the **show telephony-service** command to display only the telephony-service configuration information.

Examples

This section contains the following examples:

- MOH from an Audio File: Example, page 341
- MOH from a Live Feed: Example, page 342

**MOH from an Audio File: Example**

The following example enables music on hold and specifies the music file to use:

```
telephony-service
  moh minuet.wav
```
The following example enables MOH and additionally specifies a multicast address for the audio stream:

```
telephony-service
  moh minuet.wav
  multicast moh 239.23.4.10 port 2000
```

**MOH from a Live Feed: Example**

The following example enables MOH from an outgoing call on voice port 1/1/0 and dial peer 7777:

```
voice-port 1/1/0
  auto-cut-through
  operation 4-wire
  signal immediate
!
dial-peer voice 7777 pots
  destination-pattern 7777
  port 1/1/0
!
ephone-dn 55
  number 5555
  moh out-call 7777
```

---

**Feature History for Music on Hold**

<table>
<thead>
<tr>
<th>Cisco Unified CME Version</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.0</td>
<td>Music on hold from an audio file was introduced for external calls.</td>
</tr>
<tr>
<td>2.1</td>
<td>Music on hold from a live audio feed was introduced for external calls.</td>
</tr>
<tr>
<td>3.0</td>
<td>The ability to use a live audio feed as a multicast source was introduced.</td>
</tr>
<tr>
<td>4.0</td>
<td>• Music on hold was introduced for internal calls.</td>
</tr>
<tr>
<td></td>
<td>• The ability to disable multicast MOH per phone was introduced.</td>
</tr>
</tbody>
</table>

---

**Paging**

This feature sets up a paging number that can be called to relay audio pages to a group of designated ephones. This section describes the following topics:

- Paging Overview, page 343
- Configuring Paging, page 344
- Verifying Paging, page 348
- Examples, page 348
- Feature History for Paging, page 350
- Related Features, page 351
Paging Overview

Note For a summary of the functionality introduced in different releases, see the “Feature History for Paging” section on page 350.

Audio paging provides a one-way voice path to the phones that have been designated to receive paging. It does not have a press-to-answer option like the intercom feature. A paging group is created using a dummy ephone-dn, known as the paging ephone-dn, that can be associated with any number of local IP phones. The paging ephone-dn can be dialed from anywhere, including on-net. Figure 30 shows a paging group with two phones.

When a caller dials the paging number (ephone-dn), each idle IP phone that has been configured with the paging number automatically answers using its speakerphone mode. Displays on the phones that answer the page show the caller ID that has been set using the name command under the paging ephone-dn. When the caller finishes speaking the message and hangs up, the phones are returned to their idle states.

Once you have created two or more simple paging groups, you can unite them into combined paging groups. By creating combined paging groups, you provide phone users with the flexibility to page a small local paging group (for example, paging four phones in a store’s jewelry department) or to page a combined set of several paging groups (for example, by paging a group that consists of both the jewelry department and the accessories department).

The paging mechanism supports audio distribution using IP multicast, replicated unicast, and a mixture of both (so that multicast is used where possible, and unicast is used for specific phones that cannot be reached using multicast).

Restrictions

IP phones do not support multicast at 224.x.x.x addresses.
Configuring Paging

This procedure sets up a paging number that relays incoming pages to a group of ephones and, optionally, sets up a combined paging group made up of two or more simple paging groups.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `ephone-dn paging-dn-tag`
4. `number number`

Note that paging-dns are not assigned to phone buttons.
5. `name name`
6. `paging [ip multicast-address port udp-port-number]`
7. `exit`
8. Repeat steps Step 3 through Step 7 to create additional simple paging groups.
9. `ephone-dn paging-dn-tag`
10. `number number`
11. `name name`
12. `paging group paging-dn-tag,paging-dn-tag[[,paging-dn-tag]...]`
13. `exit`
14. `ephone phone-tag`
15. `paging-dn paging-dn-tag {multicast | unicast}`
16. `exit`
17. Repeat Step 14 through Step 16 to add additional IP phones to the paging group.

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
• Enter your password if prompted. |
| **Example:** | Router> enable |
| **Step 2** configure terminal | Enters global configuration mode. |
| **Example:** | Router# configure terminal |
| **Step 3** ephone-dn paging-dn-tag | Enters ephone-dn configuration mode.  
• `paging-dn-tag`—A unique sequence number that identifies this paging ephone-dn during all configuration tasks. This is the ephone-dn that is dialed to initiate a page. This ephone-dn is not associated with a physical phone. Range is from 1 to 288.  
**Note** Do not use the **dual-line** keyword with this command.  
Paging ephone-dns cannot be dual-line. |
| **Example:** | Router(config)# ephone-dn 42 |
| **Step 4** number number | Defines an extension number associated with the paging ephone-dn.  
This is the number that people call to initiate a page. |
| **Example:** | Router(config-ephone-dn)# number 3556 |
| **Step 5** name name | Assigns to the paging number a name to appear in caller-ID displays and directories. |
| **Example:** | Router(config-ephone-dn)# name paging4 |
## Paging

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 6</strong> paging [ip multicast-address port udp-port-number]</td>
<td>Specifies that this ephone-dn is to be used to broadcast audio paging messages to the idle IP phones that are associated with the paging dn-tag. If the optional keywords and arguments are not used, IP phones are paged individually using IP unicast transmission (to a maximum of ten IP phones). The optional keywords and arguments are as follows:</td>
</tr>
<tr>
<td>Example: Router(config-ephone-dn)# paging ip 239.1.1.10 port 2000</td>
<td>• ip multicast-address port udp-port-number—Specifies multicast broadcast using the specified IP address and UDP port. When multiple paging numbers are configured, each paging number must use a unique IP multicast address. Port 2000 is recommended because it is already used for normal nonmulticast RTP media streams between phones and the Cisco Unified CME router.</td>
</tr>
<tr>
<td><strong>Step 7</strong> exit</td>
<td>Exits ephone-dn configuration mode.</td>
</tr>
<tr>
<td>Example: Router(config-ephone-dn)# exit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong> Repeat steps Step 3 through Step 7 to create additional simple paging groups.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong> ephone-dn paging-dn-tag</td>
<td>(Optional) Enters ephone-dn configuration mode to create a paging number for a combined paging group.</td>
</tr>
<tr>
<td>Example: Router(config)# ephone-dn 42</td>
<td>• paging-dn-tag—A unique sequence number that identifies this paging ephone-dn during all configuration tasks. This is the ephone-dn that is dialed to initiate a page. This ephone-dn is not associated with a physical phone. Range is from 1 to 288.</td>
</tr>
<tr>
<td><strong>Step 10</strong> number number</td>
<td>(Optional) Defines an extension number associated with the combined group paging ephone-dn. This is the number that people call to initiate a page to the combined group.</td>
</tr>
<tr>
<td>Example: Router(config-ephone-dn)# number 3556</td>
<td></td>
</tr>
<tr>
<td><strong>Step 11</strong> name name</td>
<td>(Optional) Assigns to the combined group paging number a name to appear in caller-ID displays and directories.</td>
</tr>
<tr>
<td>Example: Router(config-ephone-dn)# name paging4</td>
<td></td>
</tr>
</tbody>
</table>

**Note** IP phones do not support multicast at 224.x.x.x addresses.
### Command or Action

**Step 12**

```markdown
paging group paging-dn-tag,[paging-dn-tag]...]
```

**Example:**

Router(config-ephone-dn)# paging group 20,21

(Optional) Sets the audio paging directory number for a combined group. The `paging group` command combines the individual paging group ephone-dns that you specify into a combined group so that a page can be sent to more than one paging group at a time. For a configuration example, see the “Examples” section on page 348.

- **paging-dn-tag**—Unique sequence number associated with the paging number for an individual paging group. List the paging-dn-tags of all the individual groups that you want to include in this combined group, separated by commas. You can include up to ten paging ephone-dn tags in this command.

**Note** Configure the `paging` command for all ephone-dns in a paging group prior to configuring the `paging group` command for that group.

**Step 13**

```markdown
exit
```

**Example:**

Router(config-ephone-dn)# exit

(Optional) Exits ephone-dn configuration mode.

**Step 14**

```markdown
ephone phone-tag
```

**Example:**

Router(config)# ephone 2

Enters ephone configuration mode to add IP phones to the paging group.

- **phone-tag**—Unique sequence number of a phone to receive audio pages when the paging ephone-dn is called.

**Step 15**

```markdown
paging-dn paging-dn-tag {multicast | unicast}
```

**Example:**

Router(config-ephone)# paging-dn 42 multicast

Associates this ephone with an ephone-dn tag that is used for a paging ephone-dn (the number that people call to deliver a page). Note that the paging ephone-dn tag is not associated with a line button on this ephone.

The paging mechanism supports audio distribution using IP multicast, replicated unicast, and a mixture of both (so that multicast is used where possible and unicast is allowed to specific phones that cannot be reached through multicast).

- **paging-dn-tag**—Unique sequence number for a paging ephone-dn.
- **multicast**—(Optional) Multicast paging for groups. By default, audio paging is transmitted to the Cisco Unified IP phone using multicast.
- **unicast**—(Optional) Unicast paging for a single Cisco Unified IP phone. This keyword indicates that the Cisco Unified IP phone is not capable of receiving audio paging through multicast and requests that the phone receive audio paging through a unicast transmission directed to the individual phone.

**Note** The number of phones supported through unicast is limited to a maximum of ten phones.
## Verifying Paging

### Step 1
Use the **show running-config** command to display the running configuration. Paging ephone-dns are listed in the ephone-dn portion of the output. Phones that belong to paging groups are listed in the ephone part of the output.

```
Router# show running-config

ephone-dn 48
  number 136
  name PagingCashiers
  paging ip 239.1.1.10 port 2000

ephone 2
  headset auto-answer line 1
  headset auto-answer line 4
  ephone-template 1
  username "FrontCashier"
  mac-address 011F.2A0.A490
  paging-dn 48
  type 7960
  no dnd feature-ring
  no auto-line
  button 1f43 2f44 3f45 4:31
```

### Step 2
Use the **show telephony-service ephone-dn** and **show telephony-service ephone** commands to display only the configuration information for ephone-dns and ephones.

### Examples

This section contains the following examples:

- **Simple Paging Group: Example, page 348**
- **Combined Paging Groups: Example, page 349**

### Simple Paging Group: Example

The following example sets up an ephone-dn for multicast paging. This example creates a paging number for 5001 on ephone-dn 22 and adds ephone 4 as a member of the paging set. Multicast is set for the paging-dn.

```
ephone-dn 22
  name Paging Shipping
  number 5001
  paging ip 239.1.1.10 port 2000
```
In this example, paging calls to 2000 are multicast to Cisco Unified IP phones 1 and 2, and paging calls to 2001 go to Cisco Unified IP phones 3 and 4. Note that the paging ephone-dns (20 and 21) are not assigned to any phone buttons.

**Combined Paging Groups: Example**

This example sets the following paging behavior:

- When extension 2000 is dialed, a page is sent to phones 1 and 2 (single paging group).
- When extension 2001 is dialed, a page is sent to phones 3 and 4 (single paging group).
- When extension 2002 is dialed, a page is sent to phones 1, 2, 3, 4, and 5 (combined paging group).

Phones 1 and 2 are included in paging ephone-dn 22 through the membership of ephone-dn 20 in the combined paging group. Phones 3 and 4 are included in paging ephone-dn 22 through membership of ephone-dn 21 in the combined paging group. Ephone 5 is directly subscribed to paging-dn 22.
Administrative and System Features

Feature History for Paging

<table>
<thead>
<tr>
<th>Cisco Unified CME Version</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.0</td>
<td>Paging was introduced.</td>
</tr>
</tbody>
</table>

Paging
Related Features

Intercom
The intercom feature is similar to paging because it allows a phone user to deliver an audio message to a phone without the called party having to answer. The intercom feature is different than paging because the audio path between the caller and the called party is a dedicated audio path and because the called party can respond to the caller. See the “Intercom” section on page 513.

Speed Dial
Phone users who make frequent pages may want to include the paging ephone-dn numbers in their list of speed-dial numbers. See the “Speed Dial” section on page 523.

Redundant Router Overview

Note
For a summary of the functionality introduced in different releases, see the “Feature History for Redundant Router” section on page 355.

Redundancy for Cisco Unified CME call control can be provided by configuring a second Cisco Unified CME router to provide services in case of the failure of the primary Cisco Unified CME router. If the primary Cisco Unified CME router fails, the secondary Cisco Unified CME router takes over and provides services seamlessly until the primary router becomes operational again.

When a phone registers to the primary router, it receives a configuration file from the primary router. Along with other information, the configuration file contains the IP addresses of the primary and secondary Cisco Unified CME routers. The phone uses these addresses to initiate a keepalive (KA) message to each router. The phone sends a KA message after every KA interval (30 seconds by default) to the router with which it is currently registered and after every two KA intervals (60 seconds by default) to the other router. The KA interval can be adjusted with the keepalive command.

If the primary router fails, a phone will not receive an acknowledgment (ACK) to its KA message to the primary router. If the phone does not get an ACK from the primary router for three consecutive KAs, it registers with the secondary Cisco Unified CME router.

During the time that the phone is registered to the secondary router, it keeps sending a KA probe to the primary router to see if it has come back up, now every 60 seconds by default or two times the normal KA interval. Once the primary Cisco Unified CME router is operating normally, the phone starts
receiving ACKs for its probes. After the phone receives ACKs from the primary router for three consecutive probes, it switches back to the primary router and reregisters with it. The reregistration of phones with the primary router is also called rehoming.

The physical setup for redundant Cisco Unified CME routers is as follows. The FXO line from the PSTN is split using a splitter. From the splitter, one line goes to the primary Cisco Unified CME router and the other goes to the secondary Cisco Unified CME router. When a call comes in on the FXO line, it is presented to both the primary and secondary Cisco Unified CME routers. The primary router is configured by default to answer the call immediately. The secondary Cisco Unified CME router is configured to answer the call after three rings using the voice-port \textbf{ring number 3} command. If the primary router is operational, it answers the call immediately and changes the call state so that the secondary router does not try to answer it. If the primary router is unavailable and does not answer the call, the secondary router sees the new call coming in and answers after three rings.

The secondary Cisco Unified CME router should be connected in some way on the LAN, either through the same switch or through another switch that may or may not be connected to the primary Cisco Unified CME router directly. As long as both routers and the phones are connected on the LAN with the appropriate configurations in place, the phones can register to whichever router is active.

Primary and secondary Cisco Unified CME routers should be configured identically, with the exception that the FXO voice port from the PSTN on the secondary router should be configured to answer after more rings than the primary router, as previously explained. The \texttt{ip source-address} command is used on both routers to specify the IP addresses of the primary and secondary routers.

**Prerequisites**

- The physical configuration of the secondary router must be as described in the “\textbf{Redundant Router Overview}” section on page 351.
- The secondary router must have a running configuration identical to that of the primary router, except for the FXO voice-port settings.
- Phones that use this feature must be configured with the \texttt{type} command, which guarantees that the appropriate phone configuration file will be present.

**Configuring a Redundant Router**

This task sets up a secondary Cisco Unified CME router to act as a backup in case the primary Cisco Unified CME router fails. Perform these steps on both the primary and secondary Cisco Unified CME routers, with the exception that the \texttt{ring number} command must be set to a higher value on the secondary router.

**SUMMARY STEPS**

1. \texttt{enable}
2. \texttt{configure terminal}
3. \texttt{telephony-service}
4. \texttt{ip source-address ip-address port port [secondary ip-address [rehome seconds]] [any-match | strict-match]}
5. \texttt{exit}
6. \texttt{voice-port slot-number/port}
7. \texttt{signal ground-start}
8. incoming alerting \{ring-only\}
9. ring number number

DETAIL STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
  * Enter your password if prompted. |
| **Example:** Router> enable | |
| **Step 2** configure terminal | Enters global configuration mode. |
| **Example:** Router# configure terminal | |
| **Step 3** telephony-service | Enters telephony-service configuration mode. |
| **Example:** Router(config)# telephony-service | |
| **Step 4** ip source-address ip-address [port port] [secondary ip-address [rehome seconds]] [any-match | strict-match] | Identifies the IP address and port number that the Cisco Unified CME router uses for IP phone registration. The default port is 2000.  
  * ip-address—Address of a Cisco Unified CME router.  
  * port port—(Optional) TCP/IP port number to use for Skinny Client Control Protocol (SCCP). Range is from 2000 to 9999. Default is 2000.  
  * secondary ip-address—(Optional) Indicates a backup Cisco Unified CME router.  
  * rehome seconds—Not used with this feature.  
  * any-match—(Optional) Disables strict IP address checking for registration. This is the default.  
  * strict-match—(Optional) Instructs the router to reject IP phone registration attempts if the IP server address used by the phone does not exactly match the source address. |
| **Example:** Router(config-telephony)# ip source-address 10.0.0.1 port 2000 secondary 10.2.2.25 | |
| **Step 5** exit | Exits telephony-service configuration mode. |
| **Example:** Router(config-telephony)# exit | |
| **Step 6** voice-port slot-number/port | Enters voice-port configuration mode. The voice port specified in this command is the FXO voice port for DID calls from the PSTN. |
| **Example:** Router(config)# voice-port 2/0 | |
### Command or Action

**Step 7**  
`s signal ground-start`  

**Example:**  
Router(config-voiceport)# signal ground-start

### Purpose

Specifies ground-start signaling for a voice port.

**Step 8**  
`incoming alerting (ring-only)`  

**Example:**  
Router(config-voiceport)# incoming alerting ring-only

### Purpose

Instructs an FXO ground-start voice port to modify its means of detecting an incoming call.  
- **ring-only**—Counts incoming rings to detect incoming calls that should be answered by the router.

**Step 9**  
`ring number number`  

**Example:**  
Router(config-voiceport)# ring number 3

### Purpose

(Optional) Sets the maximum number of rings to be detected before answering a call over an FXO voice port.  
- **number**—Number of rings detected before answering the call. Range is from 1 to 10. The default is 1.

**Note**  
To establish this port as an incoming FXO voice port for a secondary Cisco Unified CME router, set `number` to a higher number than is set on the primary router. A good setting for the secondary router is 3.

---

### Verifying a Redundant Router

**Step 1**  
Use the `show running-config` command on the primary router to verify the voice-port settings on the FXO ports and the IP address settings in the telephony-service portion of the output.

**Step 2**  
Use the `show running-config` command on the secondary router to verify that it is identical to that of the primary router.

---

### Examples

The following example is configured on the primary Cisco Unified CME router. It establishes the router at 10.5.2.78 as a secondary router. The voice port 3/0/0 is the FXO port for incoming calls from the PSTN. It is set to use ground-start signaling and detect incoming calls by counting incoming ring signals.

```plaintext
telephony-service  
ip source-address 10.0.0.1 port 2000 secondary 10.5.2.78

voice-port 3/0/0  
signal ground-start  
incoming alerting ring-only
```

The secondary Cisco Unified CME router is configured with the same commands, except that the ring number command is set to 3 instead of using the default of 1.

```plaintext
telephony-service  
ip source-address 10.0.0.1 port 2000 secondary 10.5.2.78

voice-port 3/0/0  
signal ground-start
```
Feature History for Redundant Router

<table>
<thead>
<tr>
<th>Cisco Unified CME Version</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.0</td>
<td>Redundant router capability was introduced.</td>
</tr>
</tbody>
</table>

Timeouts and Tones

This feature allows you to adjust various timeouts and tones to meet the requirements of your Cisco Unified CME system. This section contains the following topics:

- Timeouts and Tones Overview, page 355
- Configuring Timeouts and Tones, page 356
- Verifying Timeouts and Tones, page 357
- Examples, page 358
- Feature History for Timeouts and Tones, page 359
- Related Features, page 359

Timeouts and Tones Overview

For a summary of the functionality introduced in different releases, see the “Feature History for Timeouts and Tones” section on page 359.

This section discusses the following timeouts and tones:

- Busy Timeout, page 355
- Interdigit Timeout, page 355
- Ringing Timeout, page 356
- Secondary Dial Tone, page 356

Busy Timeout

The busy timeout value is the amount of time that can elapse after a transferred call reaches a busy signal before the call is disconnected.

Interdigit Timeout

The interdigit timeout is the amount of time that can elapse between the receipt of individual dialed digits before the dialing process times out and is terminated.
Ringing Timeout

The ringing timeout is the amount of time a phone can ring with no answer before returning a disconnect code to the caller. This timeout is used only for extensions that do not have no-answer call forwarding enabled. The ringing timeout prevents hung calls received over interfaces such as FXO that do not have forward-disconnect supervision.

Secondary Dial Tone

A secondary dial tone is available for Cisco Unified IP phones that are running Cisco Unified CME. The secondary dial tone is generated when a phone user dials a predefined PSTN access prefix and terminates when additional digits are dialed. An example is when a secondary dial tone is heard after the number 9 is dialed to reach an outside line.

Configuring Timeouts and Tones

This procedure sets values for various timeouts and tones used by the Cisco Unified CME system. For timeouts and tones not listed in this procedure, see the “Related Features” section on page 359.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. telephony-service
4. timeouts busy seconds
5. timeouts interdigit seconds
6. timeouts ringing seconds
7. secondary-dialtone digit-string
8. exit

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: configure terminal</td>
<td>Router# configure terminal</td>
</tr>
<tr>
<td>Step 3 telephony-service</td>
<td>Enters telephony-service configuration mode.</td>
</tr>
<tr>
<td>Example: telephony-service</td>
<td>Router(config)# telephony-service</td>
</tr>
</tbody>
</table>
### Verifying Timeouts and Tones

#### Step 1
Use the `show running-config` command to display the running configuration, including non-default settings for timeouts and tones, which will be listed in the telephony-service portion of the output.

```
telephony-service
fxo hook-flash
load 7910 P00403020214
load 7960-7940 P00305000600
load 7914 S00103020002
load 7905 CP7905040000SCCP040701A
load 7912 CP7912040000SCCP040701A
max-ephones 100
max-dn 500
ip source-address 10.153.233.41 port 2000
max-redirect 20
```

#### Command or Action | Purpose
---|---
**Step 4** timeouts busy *seconds* | Sets the amount of time after which calls are disconnected when they are transferred to busy destinations.
- *seconds*—Number of seconds. Range is from 0 to 30. Default is 10.

**Note** This command sets the busy timeout only for calls that are transferred to busy destinations and not for calls that directly dial busy destinations.

**Step 5** timeouts interdigit *seconds* | Configures the interdigit timeout value for all Cisco Unified IP phones attached to the router.

The interdigit timeout specifies the number of seconds that the system waits after the caller has entered the initial digit or a subsequent digit of the dialed string. If the timeout ends before the destination is identified, a tone sounds and the call ends. This value is important when using variable-length dial-peer destination patterns (dial plans). For more information, refer to *Dial Peer Configuration on Voice Gateway Routers*.

- *seconds*—Number of seconds before the interdigit timer expires. Range is from 2 to 120. Default is 10.

**Step 6** timeouts ringing *seconds* | Sets the duration, in seconds, for which the Cisco Unified CME system allows ringing to continue if a call is not answered. Range is from 5 to 60000. Default is 180.

**Step 7** secondary-dialtone *digit-string* | Activates a secondary dial tone when *digit-string* is dialed.

- *digit-string*—String of up to 32 digits that, when dialed, activates a secondary dial tone. Typical usage is that *digit-string* contains a single digit.

**Step 8** exit | Exits telephony-service configuration mode.
Step 2 Use the `show telephony-service` command to display only the telephony-service portion of the configuration.

Examples

This section contains the following examples:

- **Busy Timeout: Example, page 358**
- **Interdigit Timeout: Example, page 358**
- **Ringing Timeout: Example, page 358**
- **Secondary Dial Tone: Example, page 359**

**Busy Timeout: Example**
The following example sets a timeout of 20 seconds for calls that are transferred to busy destinations:

```
telephony-service
   timeouts busy 20
```

**Interdigit Timeout: Example**
The following example sets an interdigit timeout of 30 seconds:

```
telephony-service
   timeouts interdigit 30
```

**Ringing Timeout: Example**
The following example sets the ringing timeout default to 30 seconds:

```
telephony-service
   timeouts ringing 30
```
Secondary Dial Tone: Example
The following example designates the number 9 to trigger a secondary dial tone:

```
telephony-service
secondary-dialtone 9
```

Feature History for Timeouts and Tones

<table>
<thead>
<tr>
<th>Cisco Unified CME Version</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>The ability to specify an interdigit timeout was introduced.</td>
</tr>
<tr>
<td>2.0</td>
<td>The ability to specify a busy timeout was introduced.</td>
</tr>
<tr>
<td>3.0</td>
<td>The ability to specify a ringing timeout was introduced. The ability to specify a secondary dial tone was introduced.</td>
</tr>
</tbody>
</table>

Related Features

Timeouts and tones that are closely associated with other features are discussed with their respective features. For more information, refer to the following features:

- Geographically specific call tones—see the `network-locale` command and the “Network and User Locales” section.
- Phone login expiration—See the `login (telephony-service)` command and the “Call Blocking Based on Date and Time (After-Hours Toll Bar)” section on page 444.
- Call-ringing duration before calls are forwarded—See the `call-forward noan` command and the “Call Forwarding” section on page 372.
- Call-ringing duration before calls are forwarded within a hunt group—See the `timeout (ephone-hunt)` command and the “Ephone Hunt Groups” section on page 396.
- Reminder notification interval for calls on hold—See the `hold-alert` command and the “Call Hold” section on page 450.
- Reminder notification interval for parked calls—See the `park-slot` command and the “Call Park” section on page 454.
- Interval duration between keepalive messages from Cisco Unified CME to IP phones—See the `keepalive` command and the “Setting Up Basic Phone Service” section.
XML Application Programming Interface

An eXtensible Markup Language (XML) application programming interface (API) is provided to supply data from Cisco Unified CME to allow an external network management system to configure and monitor Cisco Unified CME operations. This section includes the following topics:

- XML API Overview, page 360
- Configuring the XML API, page 360
- Verifying the XML Interface, page 365
- Examples, page 366
- Troubleshooting the XML Interface, page 366
- Feature History for the XML API, page 367

**XML API Overview**

*Note*
For a summary of the functionality introduced in different releases, see the “Feature History for the XML API” section on page 367.

The Cisco IOS commands in this section allow you to specify certain parameters associated with the XML API.

In previous versions of Cisco Unified CME, the XML interface provided configuration and monitoring functions using the HTTP port. The XML interface ran under the HTTP server process, simultaneously parsing incoming XML requests on demand and processing them.

In Cisco Unified CME 4.0 and later versions, the XML interface is provided through the Cisco IOS XML Infrastructure (IXI), in which the parser and transport layers are separated from the application itself. This modularity provides scalability and enables future XML supports to be developed. In Cisco Unified CME 4.0 and later versions, all Cisco Unified CME features have XML support.

For developer information on the XML API, see the *XML Provisioning Guide for Cisco CME/SRST*.

**Configuring the XML API**

*Note*
The following Cisco IOS commands that were previously used with the XML interface are no longer valid: `log password`, `xmltest`, `xmlschema`, and `xmlthread`.

This section contains the following configuration tasks:

- Configuring XML Transport Parameters, page 361
- Configuring XML Application Parameters, page 362
- Setting Authentication for XML Access, page 363
- Setting XML Event Table Parameters, page 364
Configuring XML Transport Parameters

This task selects the XML transport method and sets parameters associated with transport.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. ip http server
4. ixti transport http
5. response size fragment-size
6. request outstanding number
7. request timeout seconds
8. no shutdown

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> ip http server</td>
<td>Enables the Cisco web browser user interface on the local Cisco Unified CME router.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# ip http server</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> ixti transport http</td>
<td>Specifies the XML transport method and enters XML-transport configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# ixti transport http</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> response size fragment-size</td>
<td>Sets the response buffer size.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(conf-xml-trans)# response size 8</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> request outstanding number</td>
<td>Sets the maximum number of outstanding requests allowed for the transport type.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(conf-xml-trans)# request outstanding 2</td>
<td></td>
</tr>
</tbody>
</table>
Configuring XML Application Parameters

This task allows you to set a response timeout for communication with the XML application that will override the setting in the transport configuration mode.

SUMMARY STEPS

1. enable
2. configure terminal
3. ixi application cme
4. response timeout {-1 | seconds}
5. no shutdown

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1 enable</strong></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2 configure terminal</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3 ixi application cme</strong></td>
<td>Specifies the Cisco Unified CME application and enters XML-application configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# ixi application cme</td>
<td></td>
</tr>
</tbody>
</table>
Setting Authentication for XML Access

This task configures authentication for Cisco Unified CME XML access.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `telephony-service`
4. `xml user user-name password password privilege-level`
5. `exit`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> <code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router&gt; enable</td>
<td>Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> <code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> <code>telephony-service</code></td>
<td>Enters telephony-service configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# telephony-service</td>
<td></td>
</tr>
</tbody>
</table>
Setting XML Event Table Parameters

This task sets the maximum number of events, or entries, that can be stored in the XML event table and the length of time that events are retained before deletion from the table. The event table is an internal buffer that stores captured and time-stamped events, such as phones registering and unregistering and extension status. One event equals one entry in the table.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. telephony-service
4. log table max-size number
5. log table retain-timer minutes
6. exit
7. exit
8. show fb-its-log
9. clear telephony-service xml-event-log

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router&gt; enable</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router# configure terminal</td>
</tr>
</tbody>
</table>
### Verifying the XML Interface

**Step 1** Use the `show running-config` command to display the running configuration.
Examples

This section contains the following examples:

- XML Transport Parameters: Example, page 366
- XML Application Parameters: Example, page 366
- XML Authentication: Example, page 366
- XML Event Table: Example, page 366

**XML Transport Parameters: Example**
The following example selects HTTP as the XML transport method:

```plaintext
ip http server
ixi transport http
response size 8
request outstanding 2
request timeout 30
no shutdown
```

**XML Application Parameters: Example**
The following example sets the application response timeout to 30 seconds.

```plaintext
ixi application cme
response timeout 30
no shutdown
```

**XML Authentication: Example**
The following example selects HTTP as the XML transport method. It allows access for user23 with the password 3Rs92uzQ, and sets up access list 99 that accepts requests from the IP address 192.168.146.72.

```plaintext
ixi transport http
ip http server

telephony-service
xml user user23 password 3Rs92uzQ 15
```

**XML Event Table: Example**
The following example sets the maximum number of entries in the XML event table to 100 and the number of minutes to retain entries at 30:

```plaintext
telephony-service
log table max-size 100
log table retain-timer 30
```

**Troubleshooting the XML Interface**

**Step 1**
To view debug messages for the Cisco Unified CME XML interface, use the `debug cme-xml` command.
Feature History for the XML API

<table>
<thead>
<tr>
<th>Cisco Unified CME Version</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.0</td>
<td>The XML API was introduced.</td>
</tr>
<tr>
<td>4.0</td>
<td>The XML API was modified and is now provided through the Cisco IOS XML infrastructure. It supports all Cisco Unified CME features. The <code>log password</code>, <code>xmltest</code>, <code>xmlschema</code>, and <code>xmlthread</code> commands were made obsolete.</td>
</tr>
</tbody>
</table>
Call-Coverage Features

This chapter describes features that can be used to provide appropriate, flexible coverage for incoming calls in a Cisco CME system. It describes the following features:

- Call Forwarding, page 372
- Call Hunt, page 379
- Call Pickup, page 385
- Call Waiting
- Cisco CME B-ACD, page 396
- Ephone Hunt Groups, page 396
- Night Service, page 420
- Overlaid Ephone-dns, page 429

Note


Call-Coverage Features Overview

Call coverage can be defined as the ability to ensure that all incoming calls to a Cisco CME system are answered by someone, even if the number that was originally dialed is busy or does not answer. Call coverage means that you ensure an adequate number of ephone-dns (virtual voice ports) for incoming calls as well as the ability for incoming calls to search among available, staffed ephone-dns until the calls are answered. This module explains Cisco CME features that you can use to provide call coverage.

Some call-coverage features allow you to designate a single number for incoming calls and several extensions to cover those incoming calls, while other features allow you to have multiple numbers covered by one or a few phone users. Table 27 summarizes the call-coverage features.

In the “single-dialed-number” group of features, Cisco Unified CME basic automatic call distribution and auto-attendant service (B-ACD) and ephone hunt groups send calls from one number to a designated pool of phone agents, while call hunt, call waiting, and call forwarding are all used to increase the chance of a call being answered by giving it another chance for a connection if the initially dialed number is not available.
In the “multiple-dialed-number” group of features, call pickup, night service, and overlaid ephone-dns provide different ways for one person to answer incoming calls to multiple numbers.

The distinction between these groups of features blurs, however, when they are used together with each other or with other Cisco CME features to provide customized call coverage for individual situations.

Any of the call-coverage features can also be combined with the use of shared lines and secondary numbers to design the call coverage plan that is best suited to your needs. For information about shared lines and secondary numbers, see the “Ephone-dns” section of the “Cisco Unified CallManager Express Overview” chapter.

### Table 27 Call-Coverage Features Summary

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Benefit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Call Forwarding</td>
<td>System diverts call to configured number on busy, no answer, all calls, or only during night-service hours.</td>
<td>Calls are automatically sent to a designated answering point under the specified conditions.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Extension 3444 is configured to send calls to extension 3555 when it is busy or does not answer.</td>
</tr>
<tr>
<td>Call Hunt</td>
<td>System matches the called number against destination patterns of ephone-dn dial peers and searches the matched ephone-dn dial peers until the call is answered or the hunt is stopped.</td>
<td>Calls automatically search for an available extension from the matching numbers that have been configured, in the order determined by the preference command until the hunt is stopped by the huntstop command.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Three ephone-dns have the same extension number, 755. One is on the manager’s phone and the others are on the assistants’ phones. Preference and huntstop can be used to make sure that calls always come to the manager’s phone first but if they can’t be answered, they will ring on the first assistant’s phone and if not answered, on the second assistant’s phone.</td>
</tr>
<tr>
<td>Call Pickup</td>
<td>A phone user can answer other ringing phones by using a soft key or by dialing a short code.</td>
<td>Calls to unstaffed phones can be answered by other phone users.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Extension 201 and 202 are both in pickup group 22. A call is received by 201, but no one is there to answer. The agent at 202 presses the GPickUp soft key to answer the call.</td>
</tr>
<tr>
<td>Call Waiting</td>
<td>System presents a second incoming call to an ephone-dn that is already connected to a call.</td>
<td>Calls to busy numbers are presented to phone users, giving them the option to answer them or let them be forwarded.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Extension 564 is in conversation when a call-waiting beep is heard. The phone display tells the phone user that the call is from extension 568 and the phone user decides to let the call go to voice mail.</td>
</tr>
</tbody>
</table>
Cisco CME B-ACD Interactive application optionally presents callers with a menu of choices before sending them to a queue for a hunt group.

Calls to a pilot number are automatically answered and distributed to appropriate hunt groups.

The DID number 555-0125 is pilot number for the XYZ Company. Incoming calls to this pilot number hear a menu of choices; they can press 1 for sales, 2 for service, or 3 to leave a message. The call is forwarded appropriately once callers make a choice.

Ephone Hunt Groups A pool of agent ephone-dns is established and incoming calls rotate among the agents.

Calls are forwarded through the pool of agents until answered or sent to a final number.

Extension 200 is a pilot number for the sales department hunt group. Extensions 213, 214, and 215 belong to sales agents in the hunt group. When a call to extension 200 is received, it proceeds through the list of agents until one answers. If all the agents are busy or do not answer, the call is sent to voice mail.

Night Service When calls arrive at specified ephone-dns during night-service hours, notification is given to particular ephones who use call pickup to answer them.

Calls to ephone-dns that are not staffed during certain hours can be answered by other phones.

Extension 7544 is the cashier’s desk but the cashier only works until 3 p.m. A call is received at 4:30 p.m. and the service manager’s phone is notified. The service manager uses call pickup to answer the call.

Overlaid Ephone-dns A number of ephone-dns can be assigned to a single button on a phone. The ephone-dns can appear on several phones.

Calls to several numbers can be answered by a single agent or multiple agents.

Extensions 451, 452, and 453 all appear on button 1 of a phone. A call to any of these numbers can be answered from button 1.

---

Table 27 Call-Coverage Features Summary

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Benefit</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco CME B-ACD</td>
<td>Interactive application optionally presents callers with a menu of choices before sending them to a queue for a hunt group.</td>
<td>Calls to a pilot number are automatically answered and distributed to appropriate hunt groups.</td>
<td>The DID number 555-0125 is pilot number for the XYZ Company. Incoming calls to this pilot number hear a menu of choices; they can press 1 for sales, 2 for service, or 3 to leave a message. The call is forwarded appropriately once callers make a choice.</td>
</tr>
<tr>
<td>Ephone Hunt Groups</td>
<td>A pool of agent ephone-dns is established and incoming calls rotate among the agents.</td>
<td>Calls are forwarded through the pool of agents until answered or sent to a final number.</td>
<td>Extension 200 is a pilot number for the sales department hunt group. Extensions 213, 214, and 215 belong to sales agents in the hunt group. When a call to extension 200 is received, it proceeds through the list of agents until one answers. If all the agents are busy or do not answer, the call is sent to voice mail.</td>
</tr>
<tr>
<td>Night Service</td>
<td>When calls arrive at specified ephone-dns during night-service hours, notification is given to particular ephones who use call pickup to answer them.</td>
<td>Calls to ephone-dns that are not staffed during certain hours can be answered by other phones.</td>
<td>Extension 7544 is the cashier’s desk but the cashier only works until 3 p.m. A call is received at 4:30 p.m. and the service manager’s phone is notified. The service manager uses call pickup to answer the call.</td>
</tr>
<tr>
<td>Overlaid Ephone-dns</td>
<td>A number of ephone-dns can be assigned to a single button on a phone. The ephone-dns can appear on several phones.</td>
<td>Calls to several numbers can be answered by a single agent or multiple agents.</td>
<td>Extensions 451, 452, and 453 all appear on button 1 of a phone. A call to any of these numbers can be answered from button 1.</td>
</tr>
</tbody>
</table>
Call Forwarding

Call forwarding allows you to divert calls to designated numbers under certain conditions. This section describes the following topics:

- Call Forwarding Overview, page 372
- Configuring Call Forwarding, page 373
- Verifying Call Forwarding, page 376
- Examples, page 377
- Troubleshooting Call Forwarding, page 378
- Feature History for Call Forwarding, page 378
- Related Features, page 379

Call Forwarding Overview

Note

For a summary of the functionality introduced in different releases, see the “Feature History for Call Forwarding” section on page 378.

Call forwarding diverts calls to a specified number under one or more of the following conditions:

- All calls—When all-call call forwarding is activated by a phone user, all incoming calls are diverted. The target destination for diverted calls can be specified in the router configuration or by the phone user with a soft key or feature access code. The most recently entered destination is recognized by Cisco CME, regardless of how it was entered.
- No answer—Incoming calls are diverted when the extension does not answer before the timeout expires. The target destination for diverted calls is specified in the router configuration.
- Busy—Incoming calls are diverted when the extension is busy and call waiting is not in effect. The target destination for diverted calls is specified in the router configuration.
- Night service—All incoming calls are automatically diverted during night-service hours. The target destination for diverted calls is specified in the router configuration.

An ephone-dn can have all four types of call forwarding defined at the same time. Each type of call forwarding can have a different forwarding destination defined in its target-number argument. If more than one type of call forwarding is in effect (is active) at one time, the precedence order for evaluating the different types is as follows:

1. Call forward night-service
2. Call forward all
3. Call forward busy and call forward no-answer

The method for exchanging call-forwarding information across a network has developed over the years. The early versions of Cisco CME, which were known as Cisco IOS Telephony Services (Cisco ITS), used a Cisco-proprietary method for call forwarding. Cisco ITS V2.1 and Cisco CME 3.0 introduced support for H.450.3, a standard protocol. The H.450.3 standard is supported by Cisco CME 3.0 and later versions but is not supported by Cisco Unified CallManager, Cisco BTS, or Cisco PGW. For a more complete discussion of network interoperability issues, see the “Call Transfer and Forwarding Across Networks” information module.
The **call-forward pattern** command is used to specify incoming patterns that are able to use the H.450.3 standard. H.450.3 capabilities are enabled globally on the router by default, but can be disabled using the **no supplementary-service h450.3** command, either globally or for individual dial peers. For information about configuring H.450.3 on a Cisco CME system, see the “Configuring Call Transfer and Call Forwarding” chapter.

### Selective Call Forwarding

You can selectively apply call forwarding for a busy or no-answer ephone-dn based on the number that callers have dialed to reach the ephone-dn: the primary number, the secondary number, or either of those numbers expanded by a dial-plan pattern.

An ephone-dn automatically creates one POTS dial peer when it is given a primary number using the **number** command. If the ephone-dn is given a secondary number, it creates a second POTS dial peer. If the **dialplan-pattern** command (under telephony-service configuration mode) is used to expand the primary and secondary numbers for ephone-dns, it creates two more dial peers, resulting in the creation of the following four dial peers for the ephone-dn:

- A POTS dial peer for the primary number
- A POTS dial peer for the secondary number
- A POTS dial peer for the primary number as expanded by the **dialplan-pattern** command
- A POTS dial peer for the secondary number as expanded by the **dialplan-pattern** command

Normally, call forwarding is applied to all dial peers created by an ephone-dn. However, if you use the **primary**, **secondary**, or **dialplan-pattern** keywords in the **call-forward busy** and **call-forward noanswer** commands, you apply those types of call forwarding only to the dial peers you have specified, based on the exact called number that was used to route the call to the ephone-dn.

For example, the following commands set up a single ephone-dn (ephone-dn 5) with four dial peers:

```plaintext
telephony-service
dialplan-pattern 1 40855501.. extension-length 4 extension-pattern 50..
ephone-dn 5
number 5066 secondary 5067
```

In this example, selective call forwarding can be applied as follows:

- Use the **primary** keyword to forward calls when callers dial 5066.
- Use the **secondary** keyword to forward calls when callers dial 5067.
- Use the **dialplan-pattern** keyword to forward calls when callers dial 4085550166 or 4085550167.

### Configuring Call Forwarding

This procedure defines the conditions and target numbers for call forwarding for individual ephone-dns, as well as certain restrictions you can set for call forwarding.

**Note**

When defining call forwarding to nonlocal numbers, it is important to note that pattern digit matching is performed before translation-rule operations. Therefore, you should specify in this command the digits actually entered by phone users before they are translated. For more information, see the “Voice Translation Rules and Profiles” section in the “Dial-Plan Support” section on page 113.
### SUMMARY STEPS

1. enable
2. configure terminal
3. telephony-service
4. call-forward pattern *pattern*
5. exit
6. ephone-dn *dn-tag* [dual-line]
7. call-forward all *target-number*
8. call-forward busy *target-number* [primary | secondary] [dialplan-pattern]
9. call-forward noan *target-number* timeout *seconds* [primary | secondary] [dialplan-pattern]
10. call-forward night-service *target-number*
11. call-forward max-length *length*
12. no forward local-calls

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
- Enter your password if prompted. |
| **Example:** |  |
| Router> enable |  |
| **Step 2** configure terminal | Enters global configuration mode. |
| **Example:** |  |
| Router# configure terminal |  |
| **Step 3** telephony-service | Enters telephony-service configuration mode. |
| **Example:** |  |
| Router(config)# |  |
| **Step 4** call-forward pattern *pattern* | Specifies the H.450.3 standard for call forwarding. Calling-party numbers that do not match the patterns defined with this command are forwarded using Cisco-proprietary call forwarding for backward compatibility (as described in the “Configuring Call Forwarding” chapter in the Cisco IOS Telephony Services V2.1 guide).  
- *pattern*—Digits to match for call forwarding using the H.450.3 standard. If an incoming calling-party number matches the pattern, it is forwarded using the H.450.3 standard. A pattern of .T forwards all calling parties using the H.450.3 standard. |
| **Example:** |  |
| Router(config-telephony)# call-forward pattern .T |  |
### Call-Coverage Features

#### Call Forwarding

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 5</strong></td>
<td><strong>exit</strong>&lt;br&gt;Enters telephony-service configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong>&lt;br&gt;Router(config-telephony)# exit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><strong>ephone-dn dn-tag [dual-line]</strong>&lt;br&gt;Enters ephone-dn configuration mode, creates an ephone-dn, and optionally assigns it dual-line status.</td>
</tr>
<tr>
<td><strong>Example:</strong>&lt;br&gt;Router(config)# ephone-dn 20</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>**number number [secondary number] [no-reg [both</td>
</tr>
<tr>
<td><strong>Example:</strong>&lt;br&gt;Router(config-ephone-dn)# number 2777 secondary 2778</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td><strong>call-forward all target-number</strong>&lt;br&gt;Forwards all calls for this extension to the specified number.</td>
</tr>
<tr>
<td><strong>Example:</strong>&lt;br&gt;Router(config-ephone-dn)# call-forward all 2411</td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td>**call-forward busy target-number [primary</td>
</tr>
<tr>
<td><strong>Example:</strong>&lt;br&gt;Router(config-ephone-dn)# call-forward busy 2513</td>
<td></td>
</tr>
</tbody>
</table>

- **dn-tag**—Unique sequence number that identifies this ephone-dn during configuration tasks. The maximum number of ephone-dns for a particular Cisco Unified CME system is version- and platform-specific. Refer to CLI help for the range of values.

- **dual-line**—(Optional) Enables an ephone-dn with one voice port and two voice channels, which supports features such as call waiting, call transfer, and conferencing with a single ephone-dn.

- **number**—String of up to 16 digits that represents a telephone or extension number to be associated with this ephone-dn.

- **secondary**—(Optional) Allows you to associate a second telephone number with an ephone-dn.

- **no-reg**—(Optional) Specifies that this number should not register with the H.323 gatekeeper. Unless you specify one of the optional keywords (**both** or **primary**) after the **no-reg** keyword, only the secondary number is not registered.

- **target-number**—Phone number to which calls are forwarded.

- **primary**—(Optional) Call forwarding is selectively applied only to the dial peer created for the primary dial peer for this ephone-dn.

- **secondary**—(Optional) Call forwarding is selectively applied only to the dial peer created for the secondary number for this ephone-dn.

- **dialplan-pattern**—(Optional) Call forwarding is selectively applied only to the dial peers created for this ephone-dn by the dial-plan pattern.
### Call-Coverage Features

#### Call Forwarding

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 10**
```bash
call-forward noan target-number timeout seconds [primary | secondary] [dialplan-pattern]
```
| Forwards calls for an extension that does not answer. |
| - **target-number**—Phone number to which calls are forwarded. |
| - **timeout seconds**—Sets the duration that a call can ring with no answer before the call is forwarded to another extension. Range is from 3 to 60000. There is no default value. |
| - **primary**—(Optional) Call forwarding is selectively applied only to the dial peer created for the primary number for this ephone-dn. |
| - **secondary**—(Optional) Call forwarding is selectively applied only to the dial peer created for the secondary number for this ephone-dn. |
| - **dialplan-pattern**—(Optional) Call forwarding is selectively applied only to the dial peers created for this ephone-dn by the dial-plan pattern. |
| **Example:**
Router(config-ephone-dn)# call-forward noan 2513 timeout 45 |

| **Step 11**
```bash
call-forward night-service target-number
```
| Automatically forwards this ephone-dn’s incoming calls to the specified number when night service is active. |
| - **target-number**—Phone number to which calls are forwarded. |
| **Note** Night service must also be configured. See the “Night Service” section on page 420. |
| **Example:**
Router(config-ephone-dn)# call-forward night-service 2879 |

| **Step 12**
```bash
call-forward max-length length
```
| (Optional) Limits the number of digits that can be entered for a target number when using the CfwdAll soft key on an IP phone. |
| - **length**—Number of digits that can be entered using the CfwdAll soft key on an IP phone. |
| **Example:**
Router(config-ephone-dn)# call-forward max-length 5 |

| **Step 13**
```bash
no forward local-calls
```
| (Optional) Specifies that local calls (calls from ephone-dns on the same Cisco Unified CME system) will not be forwarded from this extension. If this extension is busy, an internal caller hears a busy signal. If this extension does not answer, the internal caller hears ringback. |
| **Example:**
Router(config-ephone-dn)# no forward local-calls |

### Verifying Call Forwarding

| **Step 1**

Use the `show running-config` command to verify your configuration. Call forwarding is listed in the ephone-dn portion of the output.

```bash
Router# show running-config
```
| ephone-dn 1 dual-line
| ring feature secondary
| number 126 secondary 1261
| description Sales
| call-forward busy 500 secondary
| call-forward noan busy 500 secondary
| huntstop channel
| no huntstop
| no forward local-calls |

---

**Cisco Unified CallManager Express System Administrator Guide**

376
Step 2  Use the `show telephony-service ephone-dn` command to display call forwarding configuration information.

Router# `show telephony-service ephone-dn`

```plaintext
ephone-dn 2
  number 5002
  huntstop
  call-forward noan 5001 timeout 8
```

Examples

This section contains the following examples:

- Basic Call Forwarding: Example, page 377
- Call Forwarding Blocked for Local Calls: Example, page 377
- Selective Call Forwarding: Example, page 377

Basic Call Forwarding: Example
The following example sets up forwarding for extension 2777 to extension 2513 on all calls, busy, and no answer. During night service hours, calls are forwarded to a different number, extension 2879.

```plaintext
ephone-dn 20
  number 2777
  call-forward all 2513
  call-forward busy 2513
  call-forward noan 2513 timeout 45
  call-forward night-service 2879
```

Call Forwarding Blocked for Local Calls: Example
In the following example, extension 2555 is configured to not forward local calls that are internal to the Cisco CME system. Extension 2222 dials extension 2555. If 2555 is busy, the caller hears a busy tone. If 2555 does not answer, the caller hears ringback. The internal call is not forwarded.

```plaintext
ephone-dn 25
  number 2555
  no forward local-calls
  call-forward busy 2244
  call-forward noan 2244 timeout 45
```

Selective Call Forwarding: Example
The following example sets call forwarding on busy and no answer for ephone-dn 38 only for its primary number, 2777. Callers who dial 2778 will hear a busy signal if the ephone-dn is busy or ringback if there is no answer.

```plaintext
ephone-dn 38
  number 2777 secondary 2778
  call-forward busy 3000 primary
  call-forward noan 3000 primary timeout 45
```
Troubleshooting Call Forwarding

Step 1  Use the `show ephone cfa` command to list registered ephones that have call-forwarding-all (cfa) activated on one or more ephone-dns.

```
Router# show ephone cfa
ephone-1 Mac:0007.0EA6.353A TCP socket:[2] activeLine:0 REGISTERED
mediaActive:0 offhook:0 ringing:0 reset:0 reset_sent:0 paging 0 debug:0
IP:1.2.205.205 52491 Telecaster 7960  keepalive 14 max_line 6
button 1: dn 11 number 60011 cfa 60022 CH1 IDLE
button 2: dn 17 number 60017 cfa 60021 CH1 IDLE
```

Step 2  Use the `show telephony-service all` or the `show telephony-service dial-peer` command to display call forwarding configurations for ephone-dn dial peers.

```
Router# show telephony-service dial-peer
! dial-peer voice 20026 pots
  destination-pattern 5002
  huntstop
  call-forward noan 5001 timeout 45
  port 50/0/2
```

Step 3  Use the `debug ephone` commands to observe messages and states associated with an ephone. For more information, see the Cisco IOS Debug Command Reference.

Feature History for Call Forwarding

<table>
<thead>
<tr>
<th>Cisco Unified CME Version</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>Call forwarding for all calls, busy conditions, and no-answer conditions was introduced, using a Cisco-proprietary method.</td>
</tr>
<tr>
<td>2.1</td>
<td>Support was introduced for the H.450.3 standard method for call forwarding.</td>
</tr>
<tr>
<td>3.0</td>
<td>The CFwdALL (call-forward all) soft key was introduced.</td>
</tr>
<tr>
<td>3.1</td>
<td>The <code>call-forward max-length</code> command was introduced to limit the number of digits that can be entered using the CfwdAll soft key on an IP phone.</td>
</tr>
<tr>
<td>4.0</td>
<td>• Automatic call forwarding during night service was introduced.</td>
</tr>
<tr>
<td></td>
<td>• Selective call forwarding was introduced.</td>
</tr>
<tr>
<td></td>
<td>• The forwarding of local (internal) calls can be blocked.</td>
</tr>
</tbody>
</table>
Related Features

**Night Service**
Calls can be automatically forwarded during night service hours, but you must define the night-service periods, which are the dates or days and hours during which night service will be active. For instance, you may want to designate night service periods that include every weeknight between 5 p.m. and 8 a.m. and all day every Saturday and Sunday. For more information, see the “Night Service” section on page 420.

**Ephone-dn Templates**
Call-forwarding commands can be included in ephone-dn templates that are applied to individual ephone-dns. For more information, see the “Ephone-dn Templates” section on page 322.

**Feature Access Codes (FACs)**
Phone users can activate and deactivate a phone’s call-forward-all setting by using a feature access code (FAC) instead of a soft key on the phone if standard or custom FACs have been enabled for your system. The following are the standard FACs for call forward all:

- **callfwd all**—Call forward all calls. Standard FAC is **1 plus an optional target extension.
- **callfwd cancel**—Cancel call forward all calls. Standard FAC is **2.

For example, to forward all calls to extension 2534 after standard FACs are enabled, enter **12534.

For more information about FACs, see the “Feature Access Codes” section on page 325.

**Controlling Use of the Call Forward All Soft Key**
To block the functioning of the call-forward-all (CFwdAll) soft key without removing the key display, create and apply an ephone template that contains the features blocked command. For more information, see the “Feature Control” section on page 329.

To remove the call-forward-all (CFwdAll) soft key from one or more phones, create and apply an ephone template that contains the appropriate softkeys command. For more information, see the “Soft-Key Display” section on page 551.

Call Hunt

Call hunt is the ability of an incoming call to search among the ephone-dn dial peers for an available ephone-dn to answer the call. Ephone-dn dial-peer preference is used to control the order in which dial peers are searched and huntstop is used to control when the search will end. This section contains the following topics:

- Call Hunt Overview, page 380
- Verifying Call Hunt, page 382
- Verifying Call Hunt, page 382
- Examples, page 383
- Troubleshooting Call Hunt, page 384
- Feature History for Call Hunt, page 385
- Related Features, page 385
Call Hunt Overview

For a summary of the functionality introduced in different releases, see the “Feature History for Call Hunt” section on page 385.

On a voice gateway, calls are routed to dial peers based on a match between the number dialed and the destination patterns that are associated with the dial peers. Through the use of wildcards in destination patterns, multiple dial peers can match a particular called number. Call hunt is the ability to search through the dial peers that match the called number until the call is answered. Call hunt uses a technique called preference to control the order in which matching dial peers are presented to an incoming call and a technique called huntstop to direct when the search for another matching peer will end.

On voice gateways, call hunt is configured directly on the dial peers. Call hunt is described in the “Hunt Groups” section of the “Dial Peers Features and Configuration” chapter of Dial Peer Configuration on Voice Gateway Routers.

In Cisco CME systems, call hunt refers to the search that incoming calls make through the virtual dial peers that are automatically created when you define ephone-dns. These virtual dial peers are not directly configurable. The Cisco CME commands preference and huntstop commands in ephone-dn configuration mode are used instead to control call hunt for ephone-dn virtual dial peers.

To set up call hunt in Cisco CME, you first set up multiple ephone-dns that will match a called number. You can do this by assigning the same number to several primary or secondary ephone-dns or by using wildcards in ephone-dn numbers. This arrangement allows you to use several ephone-dns to provide coverage for a single number. Preference is used to control the order in which the ephone-dn dial peers are searched, and huntstop is used to determine when the search will end. These features are used together to create a call hunt group of ephone-dn dial peers.

Note

Call hunt groups consisting of ephone-dn dial peers are different from ephone hunt groups, which are described in the “Ephone Hunt Groups” section on page 396.

Ephone-dn Dial-Peer Preference

A called number can match a number that is associated with more than one ephone-dn dial peer (ephone-dn numbers can include wildcards). You can set the ephone-dn dial-peer preference for each of the matching ephone-dns to designate the order in which incoming calls should be routed to the dial peers of the matching ephone-dns. Use the preference (ephone-dn) command to assign each matching ephone-dn a preference value from 0 to 10, with 0 as the highest preference. The default is 0 if no preference is assigned. This creates a call hunt group for ephone-dn dial peers, in which calls are sent to an available extension in the group of matching numbers in the order of the extensions’ dial-peer preferences.

For example, you have two ephone-dns with the same extension number, 2680. These two ephone-dns both match the same dial-peer destination pattern because they both have the same extension number. One of the ephone-dns is on button 1 of your phone, and the other is on button 2. The ephone-dn on button 1 has been assigned a preference value of 0 (the highest value and also the default if this command is not used), and the ephone-dn on button 2 has been assigned a preference value of 1. The first call to extension 2680 is routed to button 1 because the ephone-dn on button 1 has the higher preference value. Incoming calls will always be routed to button 1 if it is free. If the ephone-dn on button 1 is occupied when a second call to extension 2680 is received by the Cisco CME system, the second call is routed to button 2.
**Huntstop**

Huntstop prevents an incoming call from rolling over to another ephone-dn if the called ephone-dn is busy or does not answer. This allows you to prevent hunt-on-busy from redirecting a call to a busy phone into a dial-peer setup with a catch-all default destination.

In ephone-dn configuration mode, huntstop is set by default. The `no huntstop` command disables huntstop to allow hunting to a nonbusy ephone-dn.

Channel huntstop works in a similar way for the two channels of a dual-line ephone-dn. If it is enabled, channel huntstop keeps incoming calls from hunting to the second channel if the first channel is busy or does not answer. This keeps the second channel free for call transfer, call waiting, or three-way conferencing. Channel huntstop also prevents situations in which a call can ring for 30 seconds on the first channel of a line with no person available to answer and then ring for another 30 seconds on the second channel before rolling over to another line.

No-huntstop call redirection is based on standard Cisco IOS voice gateway routing mechanisms.

**Configuring Call Hunt**

This procedure creates a call-hunt group of ephone-dn dial peers by setting the precedence order in which an incoming call attempts to connect with a matching ephone-dn dial peer and specifying the ephone-dn at which the hunt should stop.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `ephone-dn dn-tag [dual-line]`
4. `preference preference-order [secondary secondary-order]`
5. `no huntstop`
6. `huntstop channel`
7. Repeat Step 3 through Step 6 for the other ephone-dns to be searched in this call hunt group.

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>
Call-Coverage Features

Call Hunt

Verifying Call Hunt

Step 1 Use the show running-config command to verify your configuration. Preference and huntstop information is listed in the ephone-dn portion of the output.

Router# show running-config

ephone-dn 2 dual-line
description FrontDesk
name Receptionist
preference 1
call-forward busy 500
huntstop channel
no huntstop
Step 2

Use the `show telephony-service ephone-dn` command to display ephone-dn preference and huntstop configuration information.

```
Router# show telephony-service ephone-dn
ephone-dn 243
  number 1233
  preference 1
  huntstop
```

Examples

This section contains the following examples:

- **Ephone-dn Dial-Peer Preference: Example, page 383**
- **Huntstop Disabled: Example, page 383**
- **Channel Huntstop: Example, page 384**

**Ephone-dn Dial-Peer Preference: Example**

The following example sets an ephone-dn preference number of 2 for the primary number of the ephone-dn with dn-tag 3:

```
ephone-dn 3
  number 3001
  preference 2
```

**Huntstop Disabled: Example**

The following example shows an instance in which huntstop is not desired and is explicitly disabled. In this example, ephone 4 is configured with two lines, each with the same extension number 5001. This is done to allow the second line to provide call waiting notification for extension number 5001 when the first line is in use. Setting `no huntstop` on the first line (ephone-dn 1) allows incoming calls to hunt to the second line (ephone-dn 2) on the same phone when the ephone-dn 1 line is busy.

Ephone-dn 2 has call forwarding set to extension 6000, which corresponds to a locally attached answering machine connected to a foreign exchange station (FXS) voice port. The plain old telephone service (POTS) dial peer for extension 6000 also has the dial-peer huntstop attribute explicitly set to prevent further hunting.

```
ephone-dn 1
  number 5001
  no huntstop
  preference 1
  call-forward noan 6000

ephone-dn 2
  number 5001
  preference 2
  call-forward busy 6000
  call-forward noan 6000

ephone 4
  button 1:1 2:2
  mac-address 0030.94c3.8724
```
Channel Huntstop: Example

The following is an example that uses the huntstop channel command. It shows a dual-line ephone-dn configuration in which calls do not hunt to the second channel of any ephone-dn, but they do hunt through each ephone-dn’s channel 1 in this order: ephone-dn 10, ephone-dn 11, ephone-dn 12.

```
dial-peer voice 6000 pots
destination-pattern 6000
huntstop port 1/0/0
description answering-machine
```

ephone-dn 10 dual-line
number 1001
no huntstop
huntstop channel

ephone-dn 11 dual-line
number 1001
no huntstop
huntstop channel preference 1

ephone-dn 12 dual-line
number 1001
no huntstop
huntstop channel preference 2

Troubleshooting Call Hunt

**Step 1** Use the show telephony-service all or the show telephony-service dial-peer command to display preference and huntstop configurations for ephone-dn dial peers.

Router# show telephony-service dial-peer

```
dial-peer voice 20026 pots
destination-pattern 5002
huntstop
call-forward noan 5001 timeout 45
port 50/0/2
```

**Step 2** Use the debug ephone commands to observe messages and states associated with an ephone. For more information, see the Cisco IOS Debug Command Reference.
Feature History for Call Hunt

<table>
<thead>
<tr>
<th>Cisco Unified CME Version</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>• Ephone-dn dial-peer preference was introduced.</td>
</tr>
<tr>
<td></td>
<td>• Huntstop was introduced.</td>
</tr>
<tr>
<td>3.0</td>
<td>• Preference for secondary numbers was introduced.</td>
</tr>
<tr>
<td></td>
<td>• Channel huntstop was introduced.</td>
</tr>
</tbody>
</table>

Related Features

Dial-Peer Call Hunt and Hunt Groups

Dial peers other than ephone-dn dial peers can be directly configured as hunt groups or rotary groups, in which multiple dial peers can match incoming calls. (These are not the same as Cisco CME ephone hunt groups.) For more information, see the “Hunt Groups” section of the “Dial Peers Features and Configuration” chapter of Dial Peer Configuration on Voice Gateway Routers.

Call Pickup

Directed call pickup and pickup groups can be used to answer incoming calls from phones other than those that are ringing. The following topics are covered in this section:

- Call Pickup Overview, page 385
- Configuring Pickup Groups, page 388
- Verifying Call Pickup, page 389
- Examples, page 390
- Troubleshooting Call Pickup, page 390
- Feature History for Call Pickup, page 390
- Related Features, page 390

Call Pickup Overview

Note

For a summary of the functionality introduced in different releases, see the “Feature History for Call Pickup” section on page 390.

Cisco CME allows administrators to associate pickup groups with individual ephone-dn entries, making it easier for phone users to answer, or pick up, a call that is ringing on a different ephone-dn. If both ephone-dns are in the same pickup group, the user presses fewer keys to pick up the call.

Call pickup has the following variations:
- Call pickup, explicit ringing extension (directed call pickup)—You press the PickUp soft key and then dial the ephone-dn of the ringing telephone. You do not need to belong to a pickup group to use this method, and this method can also be used to pick up a call that is on hold on another ephone-dn.

- Call pickup, explicit group ringing extension (group pickup, different group)—You press the GPickUp soft key and then dial the pickup group number of the ringing telephone. If there is only one pickup group defined in the Cisco CME system, you need only to press the GPickUp soft key. You do not need to belong to a pickup group to use this method.

- Call pickup, local group ringing extension (local group pickup)—If the ringing telephone and the your phone are in the same pickup group, you press the GPickUp soft key and the asterisk (*) key to pick up a call on a ringing telephone.

Administrators can assign each ephone-dn independently to a maximum of one pickup group. There is no limit to the number of ephone-dns that can be assigned to a single pickup group, and there is no limit to the number of pickup groups that can be defined in a Cisco CME system.

Pickup group numbers may be of varying length, but must have unique leading digits. For example, you cannot define pickup group 17 and pickup group 177 for the same Cisco CME system because a pickup in group 17 will always be triggered before the user can enter the final 7 for 177.

Figure 31 shows four call-pickup scenarios.
**Figure 31  Call Pickup**

**Call Pickup, No Group or Unknown Group**

1. Extension 5555 rings.
2. User at phone 4 presses PickUp soft key and dials 5555.

- Phone 1
  - Extension 5555
  - Pickup group 33
- Phone 2
  - Extension 5556
  - Pickup group 33
- Phone 3
  - Extension 5557
  - Pickup group 44
- Phone 4
  - Extension 5558
  - No pickup group

**Call Pickup in the Same Group**

1. Extension 5555 rings.
2. User at phone 2 presses GPickUp soft key and * (asterisk).

- Phone 1
  - Extension 5555
  - Pickup group 33
- Phone 2
  - Extension 5556
  - Pickup group 33
- Phone 3
  - Extension 5557
  - Pickup group 44
- Phone 4
  - Extension 5558
  - No pickup group

**Call Pickup from a Different Group**

1. Extension 5555 rings.
2. User at phone 3 presses GPickUp soft key and dials 33.

- Phone 1
  - Extension 5555
  - Pickup group 33
- Phone 2
  - Extension 5556
  - Pickup group 33
- Phone 3
  - Extension 5557
  - Pickup group 44
- Phone 4
  - Extension 5558
  - No pickup group

**Call Pickup, a Single Group for All Cisco Unified CME Phones**

1. Extension 5555 rings.
2. User at phone 2 presses GPickUp soft key.

- Phone 1
  - Extension 5555
  - Pickup group 33
- Phone 2
  - Extension 5556
  - Pickup group 33

This scenario assumes that every phone in the Cisco Unified CME system is in pickup group 33, which differs slightly from the sample configuration shown to the right.
Configuring Pickup Groups

This procedure assigns ephone-dns to pickup groups.

SUMMARY STEPS

1. enable
2. configure terminal
3. ephone-dn dn-tag [dual-line]
4. pickup-group number
5. exit
6. telephony-service
7. no service directed-pickup

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router&gt; enable</td>
<td>Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> ephone-dn dn-tag [dual-line]</td>
<td>Enters ephone-dn configuration mode, creates an ephone-dn, and optionally assigns it dual-line status.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# ephone-dn 20 dual-line</td>
<td>• dn-tag—Unique sequence number that identifies this ephone-dn during configuration tasks. The maximum number of ephone-dns for a particular Cisco Unified CME system is version- and platform-specific. Refer to CLI help for the range of values.</td>
</tr>
<tr>
<td></td>
<td>• dual-line—(Optional) Enables an ephone-dn with one voice port and two voice channels, which supports features such as call waiting, call transfer, and conferencing with a single ephone-dn.</td>
</tr>
<tr>
<td><strong>Step 4</strong> pickup-group number</td>
<td>Assigns this ephone-dn to a pickup group.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-ephone-dn)# pickup-group 2345</td>
<td>• number—Digit string of up to 32 characters. Group numbers may be of varying length, but they must have unique leading digits. For example, if there is a group number 17, there cannot also be a group number 177.</td>
</tr>
</tbody>
</table>
Verifying Call Pickup

**Step 1**  Use the `show running-config` command to verify your configuration. Call pickup groups are listed in the ephone-dn portion of the output.

```
Router# show running-config

ephone-dn 34 dual-line
ring feature secondary
number 330 secondary 331
pickup-group 30
call-forward noan 500 timeout 10 secondary
huntstop channel
no huntstop
!
```

**Step 2**  Use the `show telephony-service ephone-dn` command to display call pickup configuration information.

```
Router# show telephony-service ephone-dn

ephone-dn 2
number 5002
pickup group 30
call-forward noan 5001 timeout 8
```
Examples

The following example assigns the line that has an ephone-dn tag of 55 to pickup group 2345:

```
ephone-dn 55
  number 2555
  pickup-group 2345
```

The following example globally disables directed call pickup and changes the action of the PickUp soft key to perform local group call pickup rather than directed call pickup:

```
telephony-service
  no service directed-pickup
```

Troubleshooting Call Pickup

**Step 1** Use the `debug ephone` commands to observe messages and states associated with an ephone. For more information, see the *Cisco IOS Debug Command Reference*.

Feature History for Call Pickup

<table>
<thead>
<tr>
<th>Cisco Unified CME Version</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.0</td>
<td>Call pickup groups were introduced.</td>
</tr>
<tr>
<td>3.2</td>
<td>The ability to remove or rearrange soft keys on individual phones was introduced.</td>
</tr>
<tr>
<td>4.0</td>
<td>• The ability to globally disable directed call pickup was introduced.</td>
</tr>
<tr>
<td></td>
<td>• Feature access codes for call pickup were introduced.</td>
</tr>
<tr>
<td></td>
<td>• The ability to block call pickup on individual phones was introduced.</td>
</tr>
</tbody>
</table>

Related Features

**Feature Access Codes (FACs)**

In Cisco Unified CME 4.0 and later versions, you can activate call pickup using a feature access code (FAC) instead of a soft key when standard or custom FACs have been enabled for your system. The following are the standard FACs for call pickup:

- **Pickup group**—Dial the FAC and a pickup group number to pick up a ringing call in a different pickup group than yours. Standard FAC is **4**.
- **Pickup local**—Dial the FAC to pick up a ringing call in your pickup group. Standard FAC is **3**.
- **Pickup direct**—Dial the FAC and the extension number to pick up a ringing call at any extension. Standard FAC is **5**.

For more information about FACs, see the “**Feature Access Codes**” section on page 325.
Controlling Use of the Pickup Soft Keys
To block the functioning of the group pickup (GPickUp) or local pickup (Pickup) soft key without removing the key display, create and apply an ephone template that contains the `features blocked` command. For more information, see the “Feature Control” section on page 329.

To remove the group pickup (GPickUp) or local pickup (Pickup) soft key from one or more phones, create and apply an ephone template that contains the appropriate `softkeys` command. For more information, see the “Soft-Key Display” section on page 551.

Call Waiting

Call waiting is the ability to be notified that there is a pending incoming call while a phone user is in conversation, and the ability to answer the second call or allow it to be forwarded as a no-answer call. This section discusses the following topics:

- Call Waiting Overview, page 391
- Restrictions, page 393
- Configuring Call Waiting, page 393
- Verifying Call Waiting, page 394
- Examples, page 395
- Troubleshooting Call Waiting, page 395
- Feature History for Call Waiting, page 396
- Related Features, page 396

Call Waiting Overview

For a summary of the functionality introduced in different releases, see the “Feature History for Call Waiting” section on page 396.

Call waiting allows phone users to know when another person is calling them while they are talking on the phone. Phone users hear a call-waiting tone indicating that another party is trying to reach them and, on display phones, see a display of the calling party information. Call-waiting calls to IP phones with soft keys can be answered using the Answer soft key. Call-waiting calls to analog phones configured on Cisco CME systems are answered using hookflash. When phone users answer a call-waiting call, their original call is automatically put on hold. If phone users do not respond to a call-waiting notification, the call is forwarded as specified in the `call-forward busy` command for that extension.

Call waiting for single-line ephone-dns requires two ephone-dns to handle the two calls. Call waiting on a dual-line ephone-dn requires just one ephone-dn because it uses the two channels of the ephone-dn to handle the two calls.

Overlaid ephone-dns with call waiting are configured using the `button` command and the `c` keyword. For a description of this feature and configuration steps, see the “Overlaid Ephone-dns” section on page 429.

Call waiting notification can take either of the following forms:

- Call-Waiting Beep
- Call-Waiting Ring
Call-Waiting Beep

Call-waiting beeps can be switched on or off for individual ephone-dns. You can choose to enable or disable the call-waiting beeps that are generated from and accepted by an ephone-dn.

Call-waiting beeps are enabled by default. The command for disabling an ephone-dn’s beep generation is `no call-waiting beep generate`. The command for disabling an ephone’s acceptance of call-waiting beeps is `no call-waiting beep accept`.

If an ephone-dn’s beep generation is disabled, incoming calls to the ephone-dn do not generate call-waiting beeps. If an ephone dn’s beep acceptance is disabled, the ephone-dn user will not hear beep sounds when using the ephone-dn for an active call.

Table 28 shows the possible beep behaviors of one ephone-dn calling another ephone-dn that is connected to another caller.

<table>
<thead>
<tr>
<th>Ephone-dn 1 Configuration</th>
<th>Ephone-dn 2 Configuration</th>
<th>Active Call on DN</th>
<th>Incoming Call on DN</th>
<th>Expected Behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>—</td>
<td>no call-waiting beep</td>
<td>DN 1</td>
<td>DN 2</td>
<td>No beep</td>
</tr>
<tr>
<td>no call-waiting beep</td>
<td>—</td>
<td>DN 1</td>
<td>DN 2</td>
<td>No beep</td>
</tr>
<tr>
<td>—</td>
<td>no call-waiting beep generate</td>
<td>DN 1</td>
<td>DN 2</td>
<td>No beep</td>
</tr>
<tr>
<td>—</td>
<td>no call-waiting beep accept</td>
<td>DN 1</td>
<td>DN 2</td>
<td>Beep</td>
</tr>
<tr>
<td>no call-waiting beep</td>
<td>no call-waiting beep generate</td>
<td>DN 1</td>
<td>DN 2</td>
<td>No beep</td>
</tr>
<tr>
<td>no call-waiting beep generate</td>
<td>—</td>
<td>DN 1</td>
<td>DN 1</td>
<td>No beep</td>
</tr>
<tr>
<td>no call-waiting beep accept</td>
<td>—</td>
<td>DN 1</td>
<td>DN 1</td>
<td>No beep</td>
</tr>
<tr>
<td>no call-waiting beep accept no call-waiting beep generate</td>
<td>—</td>
<td>DN 1</td>
<td>DN 1</td>
<td>No beep</td>
</tr>
<tr>
<td>no call-waiting beep generate</td>
<td>—</td>
<td>DN 1</td>
<td>DN 2</td>
<td>Beep</td>
</tr>
<tr>
<td>no call-waiting beep accept</td>
<td>—</td>
<td>DN 1</td>
<td>DN 2</td>
<td>No beep</td>
</tr>
<tr>
<td>—</td>
<td>no call-waiting beep</td>
<td>DN 1</td>
<td>DN 1</td>
<td>Beep</td>
</tr>
</tbody>
</table>

Call-Waiting Ring

Instead of the standard call waiting beep sound through the handset, you can use a short ring for call-waiting notification. Selection is made through an ephone-dn’s configuration. The default is for ephone-dns to accept call interruptions, such as call waiting, and to issue a beeping sound for notification.

To use a ring sound, you must ensure that the ephone-dn will accept call waiting. To be sure that this is the case, verify that the ephone-dn has not been configured with the `no call-waiting beep accept` command. If an ephone-dn has been configured, remove this command. After you have ensured that the ephone-dn will accept call waiting, you can configure it to issue ringing notification with the `call-waiting ring` command.
Restrictions


- The call-waiting ring option cannot be used on the Cisco Unified IP Phone 7902G, Cisco Unified IP Phone 7905G, or Cisco Unified IP Phone 7912G. Do not use the `call-waiting ring` command for ephone-dns associated with these types of phones.

- To use the call-waiting ring option, an ephone-dn cannot be configured with the `no call-waiting beep accept` command.

Configuring Call Waiting

This procedure specifies the type of call-waiting notification an ephone-dn will use.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. ephone-dn `dn-tag [dual-line]`
4. call-waiting beep [accept | generate]
5. call-waiting ring

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Router&gt; enable</code></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Router# configure terminal</code></td>
<td></td>
</tr>
</tbody>
</table>

Cisco Unified CallManager Express System Administrator Guide
**Call-Coverage Features**

**Call Waiting**

Verifying Call Waiting

**Step 1** Use the `show running-config` command to verify your configuration. Call-waiting settings are listed in the ephone-dn portion of the output. If the `no call-waiting beep generate` and the `no call-waiting beep accept` commands are configured, the `show running-config` command output will display the `no call-waiting beep` command.

```
Router# show running-config

! ephone-dn 3 dual-line
   number 126
   name Accounting
   preference 2 secondary 9
   huntstop
   huntstop channel
   call-waiting beep
```

**Step 3**

- **Command or Action**: `ephone-dn dn-tag [dual-line]`
  - **Purpose**: Enters ephone-dn configuration mode, creates an ephone-dn, and optionally assigns it dual-line status.
    - `dn-tag`—Unique sequence number that identifies this ephone-dn during configuration tasks. The maximum number of ephone-dns for a particular Cisco Unified CME system is version- and platform-specific. Refer to CLI help for the range of values.
    - `dual-line`—(Optional) Enables an ephone-dn with one voice port and two voice channels, which supports features such as call waiting, call transfer, and conferencing with a single ephone-dn.

**Step 4**

- **Command or Action**: `call-waiting beep [accept | generate]`
  - **Purpose**: Allows an ephone-dn to generate call-waiting beeps that may be received by another ephone-dn. The beep will be heard only if the other ephone-dn is configured to accept call-waiting beeps (default).
    - `accept`—Allows an ephone-dn to receive incoming call-waiting beeps.
    - `generate`—Allows an ephone-dn to generate call-waiting beeps.

**Step 5**

- **Command or Action**: `call-waiting ring`
  - **Purpose**: Allows an ephone-dn to use a ring sound for call-waiting notification.
    - **Note**: To use this command, the ephone-dn cannot be configured with the `no call-waiting beep accept` command.

---

**Example:**

- **Step 3**: `Router(config)# ephone-dn 20 dual-line`
- **Step 4**: `Router(config-ephone-dn)# no call-waiting beep accept`
- **Step 5**: `Router(config-ephone-dn)# call-waiting ring`
Step 2  Use the **show telephony-service ephone-dn** command to display call-waiting configuration information.

```bash
Router# show telephony-service ephone-dn
ephone-dn 1 dual-line
number 126 secondary 1261
preference 0 secondary 9
no huntstop
huntstop channel
call-forward busy 500 secondary
call-forward noan 500 timeout 10
call-waiting beep
```

Examples

This section contains the following examples:

- Call-Waiting Beep: Example, page 395
- Call-Waiting Ring: Example, page 395

Call-Waiting Beep: Example

In the following example, ephone-dn 10 neither accepts nor generates a beep, ephone-dn 11 does not accept a beep, and ephone-dn 12 does not generate a beep.

```bash
ephone-dn 10
no call-waiting beep
number 4410

ephone-dn 11
no call-waiting beep accept
number 4411

ephone-dn 12
no call-waiting beep generate
number 4412
```

Call-Waiting Ring: Example

The following example specifies that a short ring will indicate a call is waiting for extension 5533.

```bash
ephone-dn 20
number 5533
call-waiting ring
```

Troubleshooting Call Waiting

Step 1  Use the **debug ephone** commands to observe messages and states associated with an ephone. For more information, see the *Cisco IOS Debug Command Reference*. 

---

**Call-Coverage Features**

- Cisco Unified CallManager Express System Administrator Guide

---

**Call Waiting**

---

---

---

---

---
Feature History for Call Waiting

<table>
<thead>
<tr>
<th>Cisco Unified CME Version</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>Call waiting was introduced using two single-line ephone-dns (two line buttons).</td>
</tr>
<tr>
<td>3.0</td>
<td>Dual-line ephone-dns were introduced to support call waiting on a single button and for other features.</td>
</tr>
<tr>
<td>3.2</td>
<td>Control of call-waiting beeps was introduced.</td>
</tr>
<tr>
<td>3.2.1</td>
<td>The call-waiting ring feature was introduced. Call waiting was introduced for overlaid ephone-dns.</td>
</tr>
</tbody>
</table>

Related Features

Ephone-dn Templates
Call-waiting commands can be included in ephone-dn templates that are applied to individual ephone-dns. For more information, see the “Ephone-dn Templates” section.

Cisco CME B-ACD

Cisco Unified CME basic automatic call distribution (B-ACD) and auto-attendant (AA) service is a Tool Command Language (Tcl) application that works with Cisco Unified CME to provide the following functionality:

- Automatic answering of outside calls with greetings and menus that allow callers to select the appropriate department or to dial known extension numbers.
- Managed call queues for hunt groups that route calls for different menu options.
- Tools for obtaining call statistics.

Cisco Unified CME B-ACD is described in Cisco Unified CME B-ACD and Tcl Call-Handling Applications.

Ephone Hunt Groups

Ephone hunt groups provide the ability to direct incoming calls that dial a specific number (the ephone hunt-group pilot number) to a defined group of ephone-dns (agents). The following topics are contained within this section:

- Ephone Hunt Group Overview, page 397
- Configuring Ephone Hunt Groups, page 405
- Verifying Ephone Hunt Groups, page 411
- Examples, page 413
- Troubleshooting Ephone Hunt Groups, page 416
- Feature History for Ephone Hunt Groups, page 418
- Related Features, page 419
Ephone Hunt Group Overview

For a summary of the functionality introduced in different releases, see the “Feature History for Ephone Hunt Groups” section on page 418.

Ephone hunt groups provide the ability to direct incoming calls that dial a specific number (the ephone hunt-group pilot number) to a defined group of ephone-dns. This section discusses the following topics:

- Ephone Hunt Group Basics
- Sequential Hunt Groups
- Peer Hunt Groups
- Longest-Idle Hunt Groups
- Ephone Hunt Group Agent Availability Options

Ephone Hunt Group Basics

Each ephone hunt group can consist of up to 20 member ephone-dns (agents). Incoming calls are redirected from a hunt group pilot number to the first ephone-dn as defined by the configuration. If the first ephone-dn is busy or does not answer, the call is redirected to the next phone in the list. If the call continues to be redirected on busy or no answer from ephone-dn to ephone-dn in the list until it is answered or until the call reaches the number that was defined as the final number, the call is dropped.

The redirect from one ephone-dn to the next in the list is also known as a hop. The maximum number of redirects can be set for specific peer or longest-idle hunt groups using the hops command. In addition, the max-redirect command sets the maximum number of redirects allowed in a Cisco CME system, both inside and outside ephone hunt groups. If a call makes the maximum number of hops or redirects without being answered, the call is dropped.

There are three different kinds of ephone hunt groups. Each type of group uses a different strategy to determine the first ephone-dn that will ring for successive calls to the hunt group pilot number. Hunt group types include the following:

- Sequential ephone hunt groups—Ephone-dns always ring in the left-to-right order in which they are listed when the hunt group is defined. The first number in the list is always the first number to be tried when the pilot number is called. Maximum number of hops is not a configurable parameter for sequential ephone hunt groups.

- Peer ephone hunt groups—The first ephone-dn to ring is the number to the right of the ephone-dn that was the last to ring when the pilot number was last called. Ringing proceeds in a circular manner, left to right, for the number of hops specified in the ephone hunt group configuration.

- Longest-idle ephone hunt groups—Calls go first to the ephone-dn that has been idle the longest for the number of hops specified when the ephone hunt group was defined. The longest-idle time is determined from the last time that a phone registered, reregistered, or went on-hook.

The number that is defined as the final number for a hunt group may also be the pilot number for another hunt group (with suitable protection to avoid infinite loops). If a final number is assigned as the pilot number of a second hunt group, the pilot number of the first hunt group cannot be configured as a final number in any hunt group. If there is a third hunt group, the second hunt group cannot be configured as a final number, and so forth.
Hunt-group chains can be configured in any length, but the actual number of hops that can be reached in a chain is determined by the max-redirect command configuration. In the following example, a maximum redirect number 15 or greater must be configured for callers to reach the final 5000 number. If a lower number is configured, the call will disconnect.

```plaintext
ephone-hunt 1 sequential
  pilot 8000
  list 8001, 8002, 8003, 8004
  final 9000

ephone-hunt 2 sequential
  pilot 9000
  list 9001, 9002, 9003, 9004
  final 7000

ephone-hunt 3 sequential
  pilot 7000
  list 7001, 7002, 7003, 7004
  final 5000
```

Figure 32 on page 398 illustrates a sequential ephone hunt group, Figure 33 on page 399 illustrates a peer ephone hunt group, and Figure 34 on page 400 illustrates a longest-idle hunt group.

**Sequential Hunt Groups**

In a sequential ephone hunt group, ephone-dns always ring in the left-to-right order in which they are listed when the hunt group is defined. The first number in the list is always the first number to be tried when the pilot number is called. Maximum number of hops is not a configurable parameter for sequential ephone hunt groups.

**Figure 32  Sequential Ephone Hunt Group**

1. Any phone dials the pilot number, 5601.
2. Extension 5001, the leftmost number in the hunt group list, rings first on phone 1. If extension 5001 is busy or does not answer, the call is redirected to extension 5002 on phone 2.
3. Extension 5002, if extension 5002 on phone 2 is busy or does not answer, the call is redirected to extension 5017 on phone 3.
4. If phone 3 is busy or does not answer, the call is redirected to the final number, extension 6000, which is associated with a voice-mail server.

Any phone dials the pilot number.

Any phone dials the pilot number.
Peer Hunt Groups

In a peer ephone hunt group, the first ephone-dn to ring is the number to the right of the ephone-dn that was the last to ring when the pilot number was last called. Ringing proceeds in a circular manner, left to right, for the number of hops specified when the ephone hunt group was defined. Figure 33 illustrates a peer hunt group.

Figure 33 Peer Ephone Hunt Group

1. Any phone dials the pilot number, 5601, which is not associated with a physical phone instrument.
2. Extension 5017 on phone 3 is selected to ring first because extension 5002 was the last number to ring the last time that the pilot number was called.
3. If extension 5017 is busy or does not answer, the call is redirected to extension 5044 on phone 4 (first hop).
4. If extension 5044 is busy or does not answer, the call is redirected to extension 5001 on phone 1 (second hop).
5. If extension 5001 is busy or does not answer, the call has reached the maximum number of hops (3), and it is redirected to the final number, extension 6000, which is associated with a voice-mail server.

Any phone dials the pilot number.
Longest-Idle Hunt Groups

In a longest-idle hunt group, the algorithm for choosing the next agent to receive a call is based on a comparison of on-hook time stamps. The agent with the smallest on-hook time stamp value is chosen when the next call comes to the hunt group.

The default behavior is that an on-hook time stamp value for an agent is updated only when the agent answers a call. In Cisco CME 4.0 and later versions, the `from-ring` command can be used to specify that an on-hook time stamp should be updated when a call rings an agent as well as when a call is answered by an agent. On-hook time stamps can be displayed using the `show ephone-hunt` command.

Figure 34 illustrates a longest-idle hunt group.

Figure 34  Longest-Idle Ephone Hunt Group

1. Any phone dials the pilot number, 5601, which is not associated with a physical phone instrument.
2. Extension 5001 on phone 1 is selected to ring first because it has been idle the longest.
3. If extension 5001 does not answer, the call is redirected to extension 5002 on phone 2 because it has been idle the longest (first hop).
4. If extension 5002 does not answer, the call is redirected to extension 5044 on phone 4 because it has been idle the longest (second hop).
5. If extension 5044 does not answer, the call has reached the maximum number of hops (3), and it is redirected to the final number, extension 6000, which is associated with a voice-mail server.

Any phone dials the pilot number.

| Phone 1 | Button 1 is extension 5001 |
| Phone 2 | Button 1 is extension 5002 |
| Phone 3 | Button 1 is extension 5017 |
| Phone 4 | Button 1 is extension 5044 |

Pilot number 5601
Voice-mail server 6000

ephone-dn 88
number 5001
ephone-dn 89
number 5002
ephone-dn 90
number 5017
ephone-dn 91
number 5044
ephone 1
mac-address 1111.1111.1111
button 1:88
ephone 2
mac-address 2222.2222.2222
button 1:89
ephone 3
mac-address 3333.3333.3333
button 1:90
ephone 4
mac-address 4444.4444.4444
button 1:91
ephone-hunt 1 longest-idle
pilot 5601
list 5001, 5002, 5017, 5044
final 6000
hops 3
preference 1
timeout 30
no-reg
Ephone Hunt Group Agent Availability Options

Three similar options increase the flexibility of hunt group agents by allowing them to dynamically join and leave hunt groups or to temporarily enter a not-ready state in which they are not presented with calls. The following agent availability features are compared in Table 29 and discussed in detail following the table:

- **Dynamic Ephone Hunt Group Membership**, page 403
- **Agent Status Control**, page 403
- **Automatic Agent Status Not-Ready**, page 404

### Table 29 Comparison of Hunt Group Agent Availability Features

<table>
<thead>
<tr>
<th>Comparison Factor</th>
<th>Dynamic Membership</th>
<th>Agent Status Control</th>
<th>Automatic Agent Status Not-Ready</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Purpose</strong></td>
<td>Allows an authorized agent to join and leave hunt groups.</td>
<td>Allows an agent to manually activate a toggle to temporarily enter a not-ready state, in which hunt-group calls bypass the agent’s phone.</td>
<td>Automatically puts an agent’s phone in a not-ready state after a specified number of hunt-group calls are unanswered by the agent’s phone.</td>
</tr>
<tr>
<td><strong>Example</strong></td>
<td>Agent A joins a hunt group at 8 a.m. and takes calls until 1 p.m., when he leaves the hunt group. While Agent A is a member of the hunt group, he occupies one of the wildcard slots in the list of numbers that has been configured for the hunt group. At 1 p.m., Agent B joins the hunt group using the same wildcard slot that Agent A relinquished when he left the group.</td>
<td>Agent A takes a coffee break at 10 a.m. and puts his phone into not-ready status while he is on break. When he returns he puts his phone back into ready status and immediately starts receiving hunt-group calls again. He retained his wildcard slot while he was in not-ready status.</td>
<td>Agent B is suddenly called away from her desk before she can manually put her phone into not-ready status. After a hunt-group call is unanswered at Agent B’s phone, the phone is automatically placed in not-ready status and it is not presented with further hunt-group calls. When Agent B returns, she manually puts her phone back into ready status.</td>
</tr>
<tr>
<td><strong>Hunt-group slot availability</strong></td>
<td>An agent joining a hunt group occupies a wildcard slot in the hunt group list. An agent leaving the group relinquishes the slot, which becomes available for another agent.</td>
<td>An agent who enters the not-ready state does not give up a slot in the hunt group. The agent continues to occupy the slot even while the agent is in not-ready status.</td>
<td>An agent who enters the not-ready does not give up a slot in the hunt group. The agent continues to occupy the slot even while the agent is in not-ready status.</td>
</tr>
</tbody>
</table>
Table 29  Comparison of Hunt Group Agent Availability Features  (Continued)

<table>
<thead>
<tr>
<th>Comparison Factor</th>
<th>Dynamic Membership</th>
<th>Agent Status Control</th>
<th>Automatic Agent Status Not-Ready</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent activation method</td>
<td>An authorized agent uses a feature access code (FAC) to join a hunt group and a different FAC to leave the hunt group.</td>
<td>An agent uses the HLog soft key to toggle agent status between ready and not ready. Agents can also use the HLog ephone FAC or the HLog ephone-dn FAC to toggle between ready and not-ready if FACs have been enabled. If the HLog soft key has not been enabled in the configuration, the DND soft key can be used to put an agent in not-ready status but the agent will not receive any calls.</td>
<td>An agent who is a member of a hunt group configured with the auto logout command does not answer the specified number of calls, and the agent’s phone is automatically changed to not-ready status. The agent uses the HLog soft key or a FAC to return to ready status. If the HLog soft key or FAC has not been enabled in the configuration, the agent uses the DND soft key to return to ready status.</td>
</tr>
<tr>
<td>Configuration</td>
<td>The system administrator uses the list command to configure up to 20 wildcard slots in a hunt group and uses the ephone-hunt login command to authorize certain ephone-dns to use these wildcard slots. See Configuring Ephone Hunt Groups, page 405.</td>
<td>The system administrator uses the HLog keyword with the hunt-group logout command to provide an HLog soft key on display phones and uses the fac command to enable standard FACs or create a custom FAC. See Configuring Ephone Hunt Groups, page 405.</td>
<td>The system administrator uses the auto logout command to enable automatic agent status not-ready for a hunt group. This functionality is disabled by default. See Configuring Ephone Hunt Groups, page 405.</td>
</tr>
<tr>
<td>Optional customizations</td>
<td>The system administrator can establish custom FACs for agents to use to enter or leave a hunt group.</td>
<td>The system administrator can use the softkeys commands to change the position or prevent the display of the HLog soft key on individual phones.</td>
<td>The system administrator can use the auto logout command to specify the number of unanswered calls that will trigger an agent status change to not-ready and whether this feature applies to dynamic hunt-group members, static hunt-group members, or both. The system administrator can use the hunt-group logout command to specify whether an automatic change to not-ready status also places a phone in DND mode.</td>
</tr>
</tbody>
</table>
Dynamic Ephone Hunt Group Membership

Ephone hunt groups allow you to set up pools of extension numbers to answer incoming calls. Up to 20 wildcard slots can be entered in the list of hunt group extension numbers to allow dynamic group membership, in which authorized phone users can join a hunt group whenever a vacant wildcard slot is available and they can leave when they like. Each phone user who joins a group occupies one slot. If no slots are available, a user who tries to join a group hears a busy signal.

Allowing dynamic membership in a hunt group is a three-step process:

1. Use the list command in ephone-hunt configuration mode to specify up to 20 wildcard slots in the hunt group.

2. Use the ephone-hunt login command under each ephone-dn that should be allowed to dynamically join and leave hunt groups. Ephone-dns are disallowed from joining hunt groups by default, so you have to explicitly allow this behavior for each ephone-dn that you want to be able to log into hunt groups.

3. Use the fac standard command to enable standard FACs or the fac custom command to define custom FACs. FACs must be enabled so that agents can use them to join and leave hunt groups.

To dynamically join a hunt group, a phone user dials a standard or custom FAC for joining a hunt group. The standard FAC to join an ephone hunt group is *3. If more than one hunt group has been created that has dynamic membership, the phone user must also dial the hunt group tag number. For example, if the following hunt groups have been established, a phone user dials *324 to join the Sales ephone hunt group:

```
ephone-hunt 24 sequential
  pilot 8000
  list 8001, 8002, *, *
  description Sales Group
  final 9000

ephone-hunt 25 sequential
  pilot 7000
  list 7001, 7002, *, *
  description Service Group
  final 9000
```

To leave a hunt group, a phone user dials the standard or custom FAC for leaving a hunt group. The standard FAC to leave a hunt group is #3. See the “Related Features” section on page 419.

Note

The Dynamic Membership feature is different from the Agent Status Control feature and the Automatic Agent Status Not-Ready feature. Table 29 on page 401 compares and contrasts the features.

Agent Status Control

The Agent Status Control feature allows ephone-hunt-group agents to control whether their phones are in ready or not-ready status. A phone in ready status is available to receive calls from the hunt group. A phone in not-ready status blocks calls from the hunt group. Agents should use not-ready status for short breaks or other temporary interruptions during which they do not want to receive hunt-group calls.

Agents who put their phones into not-ready status do not relinquish their slots in the hunt group list.

Agents use the HLog soft key or the DND soft key to put a phone into not-ready status. When the HLog soft key is used to put a phone in the not-ready state, it does not receive hunt group calls but can receive other calls. If the DND soft key is used, the phone does not receive any calls until it is returned to ready status. The HLog and DND soft keys toggle the feature: if the phone is in ready status, pressing the key puts the phone in not-ready status and vice-versa.
The DND soft key is visible on phones by default, but the HLog soft key must be enabled in the configuration using the **hunt-group logout** command, which has the following options:

- **HLog**—Enables both an HLog soft key and a DND soft key on phones in the idle, seized, and connected call stages. When you press the HLog soft key, the phone is changed from ready to not-ready status or from not-ready to ready status. When the phone is in not-ready status, it does not receive calls from the hunt group, but it is still able to receive calls that do not come through the hunt group (calls that directly dial its extensions). The DND soft key is also available to block all calls to the phone if that is the preferred behavior.

- **DND**—Enables only a DND soft key on phones. The DND soft key also changes a phone from ready to not-ready status or from not-ready to ready status, but the phone does not receive any incoming calls, including those from outside hunt groups.

Phones without soft-key displays can use a FAC to toggle their status from ready to not-ready and back to ready. The **fac** command must be used to enable the standard set of FACS or to create custom FACS. The standard FAC to toggle not-ready status at the ephone-dn (extension) level is *4 and the standard FAC to toggle not-ready status at the ephone level (all ephone-dns on the phone) is *5. See the “Related Features” section on page 419.

---

**Note**

The Agent Status Control feature is different from the Dynamic Membership feature and the Automatic Agent Status Not-Ready feature. Table 29 on page 401 compares and contrasts the features.

---

**Automatic Agent Status Not-Ready**

Prior to Cisco CME 4.0, this feature was known as Automatic Hunt Group Logout. If the **auto logout** command was enabled for a hunt group, an agent phone would be placed in DND mode when a line on the phone did not answer a call for that hunt group within the time limit specified in the **timeout** command.

In Cisco CME 4.0 and later versions, the name and behavior of this feature has changed, although the Cisco IOS command name remains the same. The **auto logout** command now specifies the number of unanswered ephone hunt group calls after which the agent status of an ephone-dn is automatically changed to not-ready. You can limit Automatic Agent Status Not-Ready to dynamic hunt group members (those who log in using a wildcard slot in the **list** command) or to static hunt group members (those who are explicitly named in the **list** command), or you can apply this behavior to all hunt group members.

A related command, **hunt-group logout**, specifies whether the phones that are automatically changed to not-ready status should also be placed into DND mode or not. Phones in not-ready status do not accept calls from hunt groups, but they do accept calls that directly dial their extensions. Phones in DND mode do not accept any calls. The default if the **hunt-group logout** command is not used is that the phones that are automatically placed in not-ready status are also placed in DND mode.

Agents whose phones are automatically placed into not-ready status do not relinquish their slots in the hunt group list.

---

**Note**

The Automatic Agent Status Not-Ready feature is different from the Dynamic Membership feature and the Agent Status Control feature. Table 29 on page 401 compares and contrasts the features.
Restrictions

- The HLog soft key is available only on display phones. It is not available on Cisco Unified IP Phones 7902, 7905, and 7912; Cisco IP Communicator; and Cisco VG 224 SCCP phones.
- Shared ephone-dns cannot use the Agent Status Control or Automatic Agent Not-Ready feature.
- The Agent Status Control feature and the HLog soft key require the user locale to be set to US. To display the HLog soft key on a Cisco Unified IP Phone 7940 or Cisco Unified IP Phone 7960, change the user locale to any locale other than US and reset the phone. Then change the user locale to US and reset the phone again.

Configuring Ephone Hunt Groups

This procedure sets up an ephone hunt group and optional agent availability parameters.

SUMMARY STEPS

1. enable
2. configure terminal
3. ephone-hunt hunt-tag {peer | sequential | longest-idle}
4. pilot number [secondary number]
5. list dn-number[, dn-number...]
6. final final-number
7. hops number
8. timeout seconds[, seconds...]
9. max-timeout seconds
10. preference preference-order [secondary secondary-order]
11. no-reg [both | pilot]
12. fwd-final {orig-phone | final}
13. forward local-calls
14. secondary start [current | next | agent-position]
15. present-call {idle-phone | onhook-phone}
16. from-ring
17. description text-string
18. display-logout text-string
19. exit
20. telephony-service
21. max-redirect number
22. fac standard | custom {fac-type new-code | alias tag new-code to old-code}
23. hunt-group logout {DND | HLog}
24. exit
### Detailed Steps

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> ephone-hunt hunt-tag {peer</td>
<td>sequential</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# ephone-hunt 23 peer</td>
<td>- <strong>hunt-tag</strong>—Unique sequence number that identifies this hunt group during all configuration tasks. Range is from 1 to 100.</td>
</tr>
<tr>
<td></td>
<td>- <strong>peer</strong>—Call-hunt pattern will be peer, meaning that the first ephone-dn to ring is the number to the right of the ephone-dn that was the last to ring when the pilot number was last called. Ringing proceeds in a circular manner, left to right, for the number of hops specified when the ephone hunt group was defined.</td>
</tr>
<tr>
<td></td>
<td>- <strong>sequential</strong>—Call-hunt pattern will be sequential, meaning that ephone-dns ring in the left-to-right order in which they are listed when the hunt group is defined.</td>
</tr>
<tr>
<td></td>
<td>- <strong>longest-idle</strong>—Call-hunt pattern will be longest-idle, meaning that calls go to the ephone-dn that has been idle the longest for the number of hops specified when the ephone hunt group was defined. The longest-idle is determined from the last time that a phone registered, reregistered, or went on-hook.</td>
</tr>
<tr>
<td><strong>Step 4</strong> pilot number [secondary number]</td>
<td>Defines the pilot number, which is the number that callers dial to reach the hunt group.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-ephone-hunt)# pilot 5601</td>
<td>- <strong>number</strong>—E.164 number with a maximum length of 27 characters. The dialplan pattern can be applied to the pilot number.</td>
</tr>
<tr>
<td></td>
<td>- <strong>secondary</strong>—(Optional) Defines the number that follows as an additional pilot number for the ephone hunt group.</td>
</tr>
</tbody>
</table>
### Command or Action

<table>
<thead>
<tr>
<th>Step 5</th>
<th>list dn-number[, dn-number...]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>Router(config-ephone-hunt)# list 5001, 5002, 5017, 5028</td>
</tr>
</tbody>
</table>

defines the list of numbers to which the ephone hunt group redirects the incoming calls. There must be between two and twenty numbers in the list.

- **dn-number**—An ephone-dn primary or secondary number.

<table>
<thead>
<tr>
<th>Step 6</th>
<th>final final-number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>Router(config-ephone-hunt)# final 6000</td>
</tr>
</tbody>
</table>

Defines the last number in the ephone hunt group, after which the call is no longer redirected. This number can be an ephone-dn primary or secondary number, a voice-mail pilot number, a pilot number of another hunt group, or an FXS number.

**Note** Once a final number is defined as a pilot number of another hunt group, the pilot number of the first hunt group cannot be configured as a final number in any other hunt group.

**Note** This command is not used for ephone hunt groups that are part of a Cisco CME B-ACD service. The final destination for those groups is determined by the Cisco CME B-ACD service.

<table>
<thead>
<tr>
<th>Step 7</th>
<th>hops number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>Router(config-ephone-hunt)# hops 7</td>
</tr>
</tbody>
</table>

(Optional; peer and longest-idle hunt groups only) Sets the number of hops before a call proceeds to the final number.

- **number**—Number of hops before the call proceeds to the final ephone-dn. Range is from 2 to 20, but the value must be less than or equal to the number of extensions that are specified in the list command. Default automatically adjusts to the number of hunt group members.

<table>
<thead>
<tr>
<th>Step 8</th>
<th>timeout seconds[, seconds...]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>Router(config-ephone-hunt)# timeout 7, 10, 15</td>
</tr>
</tbody>
</table>

(Optional) Sets the number of seconds after which an unanswered call is redirected to the next number in the hunt-group list. If this command is not used, the default is the time period set by the timeouts ringing command, which has a default of 180 seconds if it is not set to another value.

- **seconds**—Number of seconds. Range is from 3 to 60000. Multiple entries can be made, separated by commas, that must correspond to the number of ephone-dns in the list command. Each number in a multiple entry specifies the time that the corresponding ephone-dn will ring before a call is forwarded to the next number in the list. If a single number is entered, it is used for the no-answer period for each ephone-dn.

**Note** Although the timeout command is optional, note that the default of 180 seconds maybe greater than you desire.
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 9</strong> max-timeout <em>seconds</em></td>
<td>(Optional) Sets the maximum combined timeout for the no-answer periods for all ephone-dns in the ephone-hunt list. The call proceeds to the final destination when this timeout expires, regardless of whether it has completed the hunt cycle. The default if this command is not used is that no combined timeout limit is set.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-ephone-hunt)# max-timeout 25</td>
<td>• <em>seconds</em>—Number of seconds. Range is from 3 to 60000.</td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
</tr>
<tr>
<td>------</td>
<td>------------------</td>
</tr>
</tbody>
</table>
| 14   | secondary start (current | (Optional) For calls that are parked by hunt group member phones, returns them to a different entry point in the hunt group (as specified in this command) if the calls are recalled from park to the secondary pilot number or transferred from park to an ephone-dn that forwards the call to the secondary pilot number.  
  - **current**—The ephone-dn that parked the call.  
  - **next**—The ephone-dn in the hunt group list that follows the ephone-dn that parked the call.  
  - **list-position**—The ephone-dn at the specified position in the list specified by the `list` command. Range is from 1 to 10. |
|      |     next |         |
|      | list-position] |         |
|      | Example: |         |
|      | Router(config-ephone-hunt)# secondary start next |         |
| 15   | present-call (idle-phone | (Optional) Presents ephone-hunt-group calls only to member phones that are idle or onhook, as specified.  
  - **idle-phone**—A call from the ephone-hunt group is presented to an ephone only if all lines on the phone are idle. This option ignores monitored lines that have been configured on the phone using the button m command.  
  - **onhook-phone**—A call from the ephone-hunt group is presented to an ephone only if the phone is in the on-hook state. When this keyword is configured, calls in the ringing or hold state that are unrelated to the hunt group do not prevent the presentation of calls from the ephone-hunt group. |
|      |     onhook-phone) |         |
|      | Example: |         |
|      | Router(config-ephone-hunt)# present-call idle-phone |         |
| 16   | from-ring | (Optional) Specifies that on-hook time stamps should be recorded when calls ring extensions as well as when calls are answered. The default is that on-hook time stamps are recorded only when calls are answered. |
|      | Example: |         |
|      | Router(config-ephone-hunt)# from-ring |         |
| 17   | description text-string | (Optional) Defines text that will appear in configuration output and on IP phones that are members of a hunt group when they receive hunt-group calls. |
|      | Example: |         |
|      | Router(config-ephone-hunt)# description Marketing Hunt Group |         |
| 18   | display-logout text-string | (Optional) Defines text that will appear on IP phones that are members of a hunt group when all the hunt-group members are in not-ready status. This string can be used to inform hunt-group members where the calls are being sent when all members are unavailable to take calls. |
|      | Example: |         |
|      | Router(config-ephone-hunt)# display-logout Night Service |         |
| 19   | exit | Exits ephone-hunt configuration mode. |
|      | Example: |         |
|      | Router(config-ephone-hunt)# exit |         |
| 20   | telephony-service | Enters telephony-service configuration mode. |
|      | Example: |         |
|      | Router(config)# telephony-service |         |
### Step 21: max-redirect number

**Example:**
```
Router(config-telephony)# max-redirect 8
```

(Optional) Sets the number of times that a call can be redirected within a Cisco CME system.

- **number**—Range is from 5 to 20. Default is 5.

**Note** This command is required if the number of hops is greater than 5.

### Step 22: fac standard | custom {fac-type new-code | alias tag new-code to old-code}

**Example:**
```
Router(config-telephony)# fac standard
```

(Optional) Enables standard FACs or creates a custom FAC or alias.

- **standard**—Enable standard FACs for all phones.
- **custom**—Create a custom FAC for a FAC type.
- **fac-type**—Type of FAC. Choose one of the following:
  - **ephone-hunt join**—(Dynamic Membership) Join an ephone-hunt group. Standard FAC is *3.
  - **ephone-hunt cancel**—(Dynamic Membership) Leave an ephone-hunt group. Standard FAC is #3.
  - **ephone-hunt hlog**—(Agent Status Control) Toggles a hunt group agent’s ephone-dn from ready to not-ready status or from not-ready to ready status. Standard FAC is *4.
  - **ephone-hunt hlog-phone**—(Agent Status Control) Toggles all the extensions on a hunt group agent’s ephone from ready to not-ready status or from not-ready to ready status. Standard FAC is *5.
- **new-code**—New FAC for the specified feature or alias.
- **alias**—Create a custom FAC for a predefined FAC or predefined FAC plus extra digits.
- **tag**—Unique identifying number for this alias.
- **old-code**—Existing FAC for which you are creating an alias. This can contain numbers in addition to the FAC.

**Note** Repeat this command to create more than one custom FAC or alias.
Step 23 Hunt-Group Logout (DND | HLog)

Example:
Router(config-telephony)# hunt-group logout
HLog

(Optional) Specifies whether agent not-ready status applies only to ephone hunt group extensions on a phone (HLog mode) or to all extensions on a phone (DND mode). Agent not-ready status can be activated by an agent using the HLog soft key or a FAC, or it can be activated automatically after the number of calls specified in the `auto logout` command are not answered.

The default if this command is not used is **DND**.

- **DND**—When phones are placed in agent not-ready status, all ephone-dns on the phone will not accept calls.
- **HLog**—Enables the display of the HLog soft key. When phones are placed in agent not-ready status, only the ephone-dns assigned to ephone hunt groups will not accept calls.

Step 24 Exit

Example:
Router(config-telephony)# exit

Exits telephony-service configuration mode.

Step 25 Ephone-Dn Dn-Tag

Example:
Router(config)# ephone-dn 29

(Optional) Enters ephone-dn configuration mode.

- **dn-tag**—Tag number for the ephone-dn to be authorized to join and leave ephone hunt groups.

Step 26 Ephone-Hunt Login

Example:
Router(config-ephone-dn)# ephone-hunt login

(Optional) Enables this ephone-dn to join and leave ephone hunt groups (dynamic membership).

Verifying Ephone Hunt Groups

Step 1 Use the `show running-config` command to verify your configuration. Ephone hunt group parameters are listed in the ephone-hunt portion of the output.

Router# show running-config

ephone-hunt 1 longest-idle
  pilot 500
  list 502, 503, *
  max-timeout 30
  timeout 10, 10, 10
  hops 2
  from-ring
  fwd-final orig-phone
  !
  ephone-hunt 2 sequential
  pilot 600
  list 621, *, 623
  final 5255348
max-timeout 10
timeout 20, 20, 20
fwd-final orig-phone
!
ephone-hunt 77 longest-idle
from-ring
pilot 100
list 101, *, 102
!

Step 2 To verify the configuration of ephone hunt group dynamic membership, use the show running-config command. Look at the ephone-hunt portion of the output to be sure at least one wildcard slot is configured. Look at the ephone-dn section to see whether particular ephone-dns are authorized to join ephone hunt groups. Look at the telephony-service section to see whether FACs are enabled.

Router# show running-config
ephone-hunt 1 longest-idle
pilot 500
list 502, 503, *
mmax-timeout 30
timeout 10, 10, 10
hops 2
from-ring
fwd-final orig-phone
!
ephone-dn 2 dual-line
number 126
preference 1
call-forward busy 500
ephone-hunt login
!
telephony-service
fac custom ephone-hunt join *3
fac custom ephone-hunt cancel #3

Step 3 Use the show ephone-hunt summary command to see configuration information for hunt groups.

Router# show ephone-hunt summary

Group 1
type: peer
pilot number: 5000
list of numbers:
5001
5002
5003
5004
5005
final number: 5006
preference: 0
timeout: 180
hops: 2
E.164 register: yes
Examples

This section contains the following examples:

- **Sequential Ephone Hunt Group: Example**, page 413
- **Peer Ephone Hunt Group: Example**, page 413
- **Longest-Idle Ephone Hunt Group: Example**, page 413
- **Longest-Idle Ephone Hunt Group Using From-Ring Option: Example**, page 414
- **Logout Display: Example**, page 414
- **Dynamic Membership: Example**, page 414
- **Agent Status Control: Example**, page 415
- **Automatic Agent Not-Ready: Example**, page 415

**Sequential Ephone Hunt Group: Example**

The following example defines a sequential ephone hunt group with the pilot number 5601 and the final number 6000, with four numbers in the list of phones that answer for the pilot number.

```
ephone-hunt 2 sequential
pilot 600
list 621, *, 623
final 5255348
max-timeout 10
timeout 20, 20, 20
fwd-final orig-phone
```

**Peer Ephone Hunt Group: Example**

The following example defines peer ephone hunt group 10 with a pilot number 450, a final number 500, and eight numbers in the list. After a call is redirected four times (makes four hops), it is redirected to the final number.

```
ephone-hunt 10 peer
pilot 450
list 451, 452, 453, 477
final 500
max-timeout 10
timeout 3, 3, 3, 3
```

**Longest-Idle Ephone Hunt Group: Example**

The following example defines longest-idle ephone hunt group 1 with a pilot number 7501 and 11 numbers in the list. After a call is redirected five times, it is redirected to the final number.

```
ephone-hunt 1 longest-idle
pilot 7501
list 7001, 7002, 7023, 7028, 7045, 7062, 7067, 7072, 7079, 7085, 7099
final 8000
preference 1
hops 5
timeout 20
no-reg
```
**Longest-Idle Ephone Hunt Group Using From-Ring Option: Example**

The following example defines longest-idle ephone hunt group 1 with a pilot number 7501, a final number 8000, and 11 numbers in the list. Because the `from-ring` command is used, on-hook time stamps will be recorded when calls ring extensions as well as when calls are answered. After a call is redirected six times (makes six hops), it is redirected to the final number, 8000. The `max-redirect` command is used to increase the number of redirects that are allowed because the number of hops (six) is larger than the default number of redirects that are allowed in the system (five).

```
ephone-hunt 1 longest-idle
  pilot 7501
  list 7001, 7002, 7023, 7028, 7045, 7062, 7067, 7072, 7079, 7085, 7099
  final 8000
  from-ring
  preference 1
  hops 6
  timeout 20

telephony-service
  max-redirect 8
```

**Logout Display: Example**

In the following example, the description is set to “Marketing Hunt Group.” This information will be shown in the configuration output and also on the display of IP phones that are receiving calls from this hunt group. The display-logout message is set to “Night Service,” which will be displayed on IP phones that are members of the hunt group when all the members are logged out.

```
ephone-hunt 17 sequential
  pilot 3000
  list 3011, 3021, 3031
  timeout 10
  final 7600
  description Marketing Hunt Group
  display-logout Night Service
```

**Dynamic Membership: Example**

The following example creates four ephone-dns and a hunt group that includes the first ephone-dn and two wildcard slots. The last three ephone-dns are enabled for group hunt dynamic membership. Each of them can join and leave the hunt group whenever one of the wildcard slots is available. Standard FACs have been enabled, and the agents use standard FACs to join (*3) and leave (#3) the hunt group. You can also use the `fac` command to create custom FACs for these actions if you prefer.

```
ephone-dn 22
  number 4566

ephone-dn 24
  number 4568
  ephone-hunt login

ephone-dn 25
  number 4569
  ephone-hunt login

ephone-dn 26
  number 4570
  ephone-hunt login

ephone-hunt 1 peer
  list 4566,*,*```
timeout 10
final 7777

telephony-service
fac standard

**Agent Status Control: Example**
The following example sets up a peer ephone hunt group. It also establishes the appearance and order of soft keys for phones that are configured with ephone-template 7. These phones will have the HLog key available when they are idle, when they have seized a line, or when they are connected to a call. Phones without soft keys can use the standard HLog codes to toggle ready and not-ready status.

```plaintext
ephone-hunt 10 peer
    pilot 450
    list 451, 452, 453, 477
    final 500
    timeout 45

telephony-service
    hunt-group logout HLog
    fac standard

ephone-template 7
    softkeys connected Endcall Hold Transfer HLog
    softkeys idle Newcall Redial Pickup Cfwdall HLog
    softkeys seized Endcall Redial Pickup Cfwdall HLog
```

**Automatic Agent Not-Ready: Example**
The following example enables automatic status change to not-ready after one unanswered hunt group call (the default) for both dynamic and static hunt group members (the default). It also specifies that the phones which are automatically put into not-ready status should only be blocked from further hunt-group calls and that they should be able to receive calls that directly dial their extensions.

```plaintext
ephone-hunt 3 peer
    pilot 4200
    list 1001, 1002, 1003
    timeout 10
    auto logout
    final 4500

telephony-service
    hunt-group logout HLog
```

The following example enables automatic status change to not-ready after two unanswered hunt group calls for any ephone-dn that dynamically logs in to the hunt group using the wildcard slot in the hunt group list. Phones that are automatically placed in not-ready status when they do not answer two hunt-group calls are also placed into DND status (they will also not accept directly dialed calls).

```plaintext
ephone-hunt 3 peer
    pilot 4200
    list 1001, 1002, *
    timeout 10
    auto logout 2 dynamic
    final 4500

telephony-service
    hunt-group logout DND
```
Troubleshooting Ephone Hunt Groups

Step 1  Use the `show ephone-hunt` command for detailed information about hunt groups, including dial-peer tag numbers and hunt-group agent status. This command also displays the dial-peer tag numbers of all ephone-dns that have joined dynamically and are members of the group at the time that the command is run.

Router# show ephone-hunt

Group 1
  type: peer
  pilot number: 450, peer-tag 20123
  list of numbers:
    451, aux-number A450A0900, # peers 5, logout 0, down 1
    peer-tag dn-tag rna login/logout up/down
    [20122 42 0 login up ]
    [20121 41 0 login up ]
    [20120 40 0 login up ]
    [20119 30 0 login up ]
    [20118 29 0 login down]
    452, aux-number A450A0901, # peers 4, logout 0, down 0
    peer-tag dn-tag rna login/logout up/down
    [20127 45 0 login up ]
    [20126 44 0 login up ]
    [20125 43 0 login up ]
    [20124 31 0 login up ]
    453, aux-number A450A0902, # peers 4, logout 0, down 0
    peer-tag dn-tag rna login/logout up/down
    [20131 48 0 login up ]
    [20130 47 0 login up ]
    [20129 46 0 login up ]
    [20128 32 0 login up ]
    477, aux-number A450A0903, # peers 1, logout 0, down 0
    peer-tag dn-tag rna login/logout up/down
    [20132 499 0 login up ]
  preference: 0
  preference (sec): 7
  timeout: 3, 3, 3, 3
  max timeout : 10
  hops: 4
  next-to-pick: 1
  E.164 register: yes
  auto logout: no
  stat collect: no

Group 2
  type: sequential
  pilot number: 601, peer-tag 20098
  list of numbers:
    123, aux-number A601A0200, # peers 1, logout 0, down 0
    peer-tag dn-tag rna login/logout up/down
    [20097 56 0 login up ]
    622, aux-number A601A0201, # peers 3, logout 0, down 0
    peer-tag dn-tag rna login/logout up/down
    [20101 112 0 login up ]
    [20100 111 0 login up ]
    [20099 110 0 login up ]
    623, aux-number A601A0202, # peers 3, logout 0, down 0
    peer-tag dn-tag rna login/logout up/down
    [20104 122 0 login up ]
    [20103 121 0 login up ]
    [20102 120 0 login up ]
    *, aux-number A601A0203, # peers 1, logout 0, down 1
### Call-Coverage Features

#### Ephone Hunt Groups

<table>
<thead>
<tr>
<th>peer-tag</th>
<th>dn-tag</th>
<th>rna</th>
<th>login/logout</th>
<th>up/down</th>
</tr>
</thead>
<tbody>
<tr>
<td>20105</td>
<td>0</td>
<td>0</td>
<td>-</td>
<td>down</td>
</tr>
</tbody>
</table>

*, aux-number A601A0204, # peers 1, logout 0, down 1

<table>
<thead>
<tr>
<th>peer-tag</th>
<th>dn-tag</th>
<th>rna</th>
<th>login/logout</th>
<th>up/down</th>
</tr>
</thead>
<tbody>
<tr>
<td>20106</td>
<td>0</td>
<td>0</td>
<td>-</td>
<td>down</td>
</tr>
</tbody>
</table>

final number: 5255348

preference: 0

preference (sec): 9

timeout: 5, 5, 5, 5, 5

max timeout : 40

fwd-final: orig-phone

E.164 register: yes

auto logout: no

stat collect: no

**Group 3**

type: longest-idle

pilot number: 100, peer-tag 20142

list of numbers:

<table>
<thead>
<tr>
<th>peer-tag</th>
<th>dn-tag</th>
<th>rna</th>
<th>login/logout</th>
<th>up/down</th>
</tr>
</thead>
<tbody>
<tr>
<td>20141</td>
<td>132</td>
<td>0</td>
<td>login</td>
<td>down</td>
</tr>
<tr>
<td>20140</td>
<td>131</td>
<td>0</td>
<td>login</td>
<td>down</td>
</tr>
<tr>
<td>20139</td>
<td>130</td>
<td>0</td>
<td>login</td>
<td>down</td>
</tr>
</tbody>
</table>

*, aux-number A100A9701, # peers 1, logout 0, down 1

on-hook time stamp 7616, off-hook agents=0

<table>
<thead>
<tr>
<th>peer-tag</th>
<th>dn-tag</th>
<th>rna</th>
<th>login/logout</th>
<th>up/down</th>
</tr>
</thead>
<tbody>
<tr>
<td>20143</td>
<td>0</td>
<td>0</td>
<td>-</td>
<td>down</td>
</tr>
</tbody>
</table>

101, aux-number A100A9700, # peers 3, logout 0, down 3

on-hook time stamp 7616, off-hook agents=0

<table>
<thead>
<tr>
<th>peer-tag</th>
<th>dn-tag</th>
<th>rna</th>
<th>login/logout</th>
<th>up/down</th>
</tr>
</thead>
<tbody>
<tr>
<td>20141</td>
<td>132</td>
<td>0</td>
<td>login</td>
<td>down</td>
</tr>
<tr>
<td>20140</td>
<td>131</td>
<td>0</td>
<td>login</td>
<td>down</td>
</tr>
<tr>
<td>20139</td>
<td>130</td>
<td>0</td>
<td>login</td>
<td>down</td>
</tr>
</tbody>
</table>

*, aux-number A100A9701, # peers 1, logout 0, down 1

on-hook time stamp 7616, off-hook agents=0

<table>
<thead>
<tr>
<th>peer-tag</th>
<th>dn-tag</th>
<th>rna</th>
<th>login/logout</th>
<th>up/down</th>
</tr>
</thead>
<tbody>
<tr>
<td>20143</td>
<td>0</td>
<td>0</td>
<td>-</td>
<td>down</td>
</tr>
</tbody>
</table>

102, aux-number A100A9702, # peers 2, logout 0, down 2

on-hook time stamp 7616, off-hook agents=0

<table>
<thead>
<tr>
<th>peer-tag</th>
<th>dn-tag</th>
<th>rna</th>
<th>login/logout</th>
<th>up/down</th>
</tr>
</thead>
<tbody>
<tr>
<td>20145</td>
<td>142</td>
<td>0</td>
<td>login</td>
<td>down</td>
</tr>
<tr>
<td>20144</td>
<td>141</td>
<td>0</td>
<td>login</td>
<td>down</td>
</tr>
</tbody>
</table>

all agents down!

preference: 0

preference (sec): 7

timeout: 100, 100, 100

hops: 0

E.164 register: yes

auto logout: no

stat collect: no

---

**Step 2** Use the `debug ephone` commands to observe messages and states associated with an ephone. For more information, see the *Cisco IOS Debug Command Reference*. 

---

*Cisco Unified CallManager Express System Administrator Guide*
# Feature History for Ephone Hunt Groups

<table>
<thead>
<tr>
<th>Cisco Unified CME Version</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.0</td>
<td>Peer and sequential ephone hunt groups were introduced.</td>
</tr>
<tr>
<td>3.1</td>
<td>Secondary pilot numbers were introduced.</td>
</tr>
<tr>
<td>3.2</td>
<td>Longest-idle hunt groups were introduced.</td>
</tr>
</tbody>
</table>
| 3.2.1                     | • Maximum number of hunt groups in a system was increased to 20.  
• Automatic logout capability was introduced. |
| 4.0                       | • Maximum number of hunt groups in a system was increased from 20 to 100 and maximum number of agents in a hunt group was increased from 10 to 20.  
• Maximum number of hops automatically adjusts to the number of agents.  
• A description can be added to phone displays and configuration output to provide hunt group information associated with ringing and answered calls.  
• A configurable message can be displayed on agent phones when all agents are in not-ready status to advise the destination to which calls are being forwarded or other useful information.  
• No-answer timeouts can be set individually for each ephone-dn in the list and a cumulative no-answer timeout can be set for all ephone-dns.  
• Automatic logout trigger criterion was changed from exceeding the specified timeout to exceeding the specified number of calls. The name of this feature was changed from automatic logout to automatic agent status not-ready.  
• Dynamic hunt group membership is introduced. Agents can join and leave hunt groups whenever a wildcard slot is available.  
• Agent status control using an HLog soft key or feature access code (FAC) is introduced. Agents can put their lines into not-ready status to temporarily block hunt group calls without relinquishing their slots in the group.  
• Calls can be blocked from agent phones that are not idle or on hook.  
• Calls that are not answered by the hunt group can be returned to the party who transferred them into the hunt group.  
• Calls parked by hunt group agents can be returned to a different entry point.  
• (Sequential hunt groups only) Local calls to a hunt group can be restricted so that they will not be forwarded past the initial agent that is rung.  
• (Longest-idle hunt groups only) A new command, the **from-ring** command, specifies that on-hook time stamps should be updated when a call rings an agent as well as when a call is answered by an agent. |
Related Features

**Feature Access Codes (FACs)**
Dynamic membership allows agents at authorized ephones to join or leave an ephone hunt group using a feature access code (FAC) after standard or custom FACs have been enabled. The following are the standard FACs that are used for dynamic hunt group membership:

- Join ephone-hunt group—*3 plus optional hunt group tag number
- Leave ephone-hunt group—#3

The agent status control feature and the automatic agent status not-ready feature can use FACs to toggle agent status from ready to not-ready or from not-ready to ready after standard or custom FACs have been enabled. The following are the standard FACs that are used to toggle agent status:

- Toggle hunt group agent ready/not-ready status for an ephone-dn—*4
- Toggle hunt group agent ready/not-ready status for all ephone-dns on an ephone—*5

For more information about FACs, see the “Feature Access Codes” section on page 325

**Soft Key Control**
If the **hunt-group logout** command is used with the **HLog** keyword, the HLog soft key appears on phones during the idle, connected, and seized call states. The HLog soft key is used to toggle an agent from ready to not-ready status or from not-ready to ready status. To move or remove the HLog soft key on one or more phones, create and apply an ephone template that contains the appropriate **softkeys** commands.

For more information, see the “Soft-Key Display” section on page 551.

**Ephone-dn Templates**
The **ephone-hunt login** command authorizes an ephone-dn to dynamically join and leave an ephone hunt group. It can be included in an ephone-dn template that is applied to one or more individual ephone-dns.

For more information, see the “Ephone-dn Templates” section on page 322.

**Ephone Hunt Group Statistics Reports**
Several different types of statistics can help you track whether your current ephone hunt groups are meeting your call-coverage needs. These statistics can be displayed on-screen or written to files.

For more information, see the “Cisco Unified CME Basic Automatic Call Distribution and Auto-Attendant Service” chapter in *Cisco Unified CME B-ACD and Tcl Call-Handling Applications*.

**Do Not Disturb**
The Do Not Disturb (DND) feature can be used as an alternative to the HLog function for preventing incoming calls from ringing on a phone. The difference is that HLog prevents only hunt group calls from ringing, while DND prevents all calls from ringing. For more information, see the “Do Not Disturb” section on page 504.
Night Service

During the hours that have been defined in the router configuration as night-service hours, the night service feature provides the ability to alert specified phones that calls are ringing at certain ephone-dns that are designated as night-service ephone-dns. This section discusses the following topics:

- Night Service Overview, page 420
- Configuring Night Service, page 422
- Verifying Night Service, page 425
- Examples, page 427
- Feature History for Night Service, page 428
- Related Features, page 428

Night Service Overview

Note

For a summary of the functionality introduced in different releases, see the “Feature History for Night Service” section on page 428.

The night-service feature allows you to provide coverage for unstaffed extensions during hours that you designate as “night-service” hours. During the night-service hours, calls to the designated extensions (known as night-service ephone-dns or night-service lines) send a special “burst” ring to phones that have been specified to receive this special ring (the phones are known as night-service phones). Phone users at the night-service phones can then use the call-pickup feature to answer the incoming calls from the night-service ephone-dns (Figure 35).

For example, the night-service feature can allow an employee working after hours to intercept and answer calls that are presented to an unattended receptionist’s phone. This feature is useful for sites at which all incoming public switched telephone network (PSTN) calls have to be transferred by a receptionist because the PSTN connection to the Cisco CME system does not support Direct Inward Dialing (DID). When a call arrives at the unattended receptionist’s phone during hours that are specified as night service, a ring burst notifies a specified set of phones of the incoming call. A phone user at any of the night-service phones can intercept the call using the call-pickup feature. Night-service call notification is sent every 12 seconds until the call is either answered or aborted.

If optionally configured, night service can be manually toggled on and off from any phone that has a line that is designated as a night-service line. When night service is active, a message is displayed on the night-service phones.

Night service requires that you define the following parameters:

1. Night-service time period—Day or date and hours during which night service is active. Step 4 through Step 8 in the following procedure define the night-service period.

2. Night-service extensions (ephone-dns)—When a night-service extension receives an incoming call during the night-service period, night-service notification is triggered. Step 12 in the following procedure specifies night service for an ephone-dn.

3. Night-service notification phones (ephones)—Night-service notification phones are alerted with a distinctive ring when incoming calls are received on night-service lines during the night-service time period. The night-service notification phone user can answer the call using call pickup or group
call pickup. **Step 15** in the following procedure assigns night-service notification to a phone. This phone receives a distinctive alerting ring and notification display when a night-service extension receives an incoming call.

4. (Optional) Night-service toggle code—A code to allow night-service treatment to be manually toggled off and on from any phone that has a line assigned to night service. Prior to Cisco CME 3.3, using the night-service code turned night service on or off only for ephone-dns on the phone at which the code was entered. In Cisco CME 3.3 and later versions, using the night-service code at any phone with a night-service ephone-dn turns night service on or off for all phones with night-service ephone-dns. in the following procedure defines a night-service toggle code.

Figure 35 illustrates night service.

**Figure 35  Night Service**

1. Extension 1000 has been designated as a night-service extension (ephone-dn). When extension 1000 receives an incoming call during a night-service period, phone 5 rings and notification is made to the night-service phones.

2. Phones 14 and 15 have been designated as night-service phones. When phone 5 starts ringing, phones 14 and 15 ring once and display “Night Service 1000.” The incoming call on extension 1000 can be answered from phone 14 or phone 15 using call pickup.

```
telephony-service
night-service day fri 17:01 17:00
night-service day sat 17:01 17:00
night-service day sun 17:01 07:59
night-service date jan 1 00:00 00:00
night-service code *1234

ephone-dn 1
  number 1000
  night-service bell

ephone-dn 10
  number 1010

ephone-dn 11
  number 1011

ephone 5
  mac-address 1111.2222.0001
  button 1:1

ephone 14
  mac-address 1111.2222.0002
  button 1:10
  night-service bell

ephone 15
  mac-address 1111.2222.0003
  button 1:11
  night-service bell
```

Phone 5
Button 1 is extension 1000
Extension 1000 is a night-service extension

Phone 14
Button 1 is extension 1010
Phone 14 is a night-service phone

Phone 15
Button 1 is extension 1011
Phone 15 is a night-service phone
Configuring Night Service

This procedure defines night-service hours and an optional night-service code, as well as the ephone-dns that will trigger the notification process and the ephones that will receive notification.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. telephony-service
4. night-service day day start-time stop-time
5. night-service date month date start-time stop-time
6. night-service everyday start-time stop-time
7. night-service weekday start-time stop-time
8. night-service weekend start-time stop-time
9. night-service code digit-string
10. exit
11. ephone-dn dn-tag
12. night-service bell
13. exit
14. ephone phone-tag
15. night-service bell

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>telephony-service</td>
<td>Enters telephony-service configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# telephony-service</td>
<td></td>
</tr>
</tbody>
</table>
### Command or Action

#### Step 4

```bash
night-service day day start-time stop-time
```

**Example:**
```
Router(config-telephony)# night-service day mon 19:00 07:00
```

**Purpose:**
Defines a recurring time period associated with a day of the week during which night service is active.
- **day**—Day of the week abbreviation. The following are valid day abbreviations: **sun**, **mon**, **tue**, **wed**, **thu**, **fri**, **sat**.
- **start-time** **stop-time**—Beginning and ending times for night service, in an HH:MM format using a 24-hour clock. If the stop time is a smaller value than the start time, the stop time occurs the day following the start time. For example, **“mon 19:00 07:00”** means “from Monday at 7 p.m. until Tuesday at 7 a.m.”

#### Step 5

```bash
night-service date month date start-time stop-time
```

**Example:**
```
Router(config-telephony)# night-service date jan 1 00:00 00:00
```

**Purpose:**
Defines a recurring time period associated with a month and date during which night service is active.
- **month**—Month abbreviation. The following are valid month abbreviations: **jan**, **feb**, **mar**, **apr**, **may**, **jun**, **jul**, **aug**, **sep**, **oct**, **nov**, **dec**.
- **date**—Date of the month. Range is from 1 to 31.
- **start-time** **stop-time**—Beginning and ending times for night service, in an HH:MM format using a 24-hour clock. The stop time must be greater than the start time. The value 24:00 is not valid. If 00:00 is entered as an stop time, it is changed to 23:59. If 00:00 is entered for both start time and stop time, calls are blocked for the entire 24-hour period on the specified date.

#### Step 6

```bash
night-service everyday start-time stop-time
```

**Example:**
```
Router(config-telephony)# night-service everyday 1200 1300
```

**Purpose:**
Defines a recurring night-service time period to be in effect on all days.
- **start-time** **stop-time**—Beginning and ending times for night service, in an HH:MM format using a 24-hour clock. If the stop time is a smaller value than the start time, the stop time occurs the day following the start time. For example, **“19:00 07:00”** means “from 7 p.m. to 7 a.m. the next morning.” The value 24:00 is not valid. If 00:00 is entered as a stop time, it is changed to 23:59. If 00:00 is entered for both start time and stop time, the night service feature will be activated for the entire 24-hour period.
### Step 7
**Command or Action:**
```
night-service weekday start-time stop-time
```
**Example:**
```
Router(config-telephony)# night-service weekday 1700 0700
```
**Purpose:** Defines a recurring night-service time period to be in effect on all weekdays.
- *start-time stop-time*—Beginning and ending times for night service, in an HH:MM format using a 24-hour clock. If the stop time is a smaller value than the start time, the stop time occurs the day following the start time. For example, “19:00 07:00” means “from 7 p.m. to 7 a.m. the next morning.” The value 24:00 is not valid. If 00:00 is entered as a stop time, it is changed to 23:59. If 00:00 is entered for both start time and stop time, the night service feature will be activated for the entire 24-hour period.

### Step 8
**Command or Action:**
```
night-service weekend start-time stop-time
```
**Example:**
```
Router(config-telephony)# night-service weekend 00:00 00:00
```
**Purpose:** Defines a recurring night-service time period to be in effect on all weekend days. Weekend is defined as Saturday and Sunday.
- *start-time stop-time*—Beginning and ending times for night service, in an HH:MM format using a 24-hour clock. If the stop time is a smaller value than the start time, the stop time occurs the day following the start time. For example, “19:00 07:00” means “from 7 p.m. to 7 a.m. the next morning.” The value 24:00 is not valid. If 00:00 is entered as a stop time, it is changed to 23:59. If 00:00 is entered for both start time and stop time, the night service feature will be activated for the entire 24-hour period.

### Step 9
**Command or Action:**
```
night-service code digit-string
```
**Example:**
```
Router(config-telephony)# night-service code *6483
```
**Purpose:** Designates a code that can be dialed from any night-service line (ephone-dn) to toggle night service on and off for all lines that have been assigned to night service in the system. The night-service state is indicated in a display message on phones that have active night-service lines.
- *digit-string*—String of up to 16 keypad digits. The code must begin with an asterisk (*).

### Step 10
**Command or Action:**
```
exit
```
**Example:**
```
Router(config-telephony)# exit
```
**Purpose:** Exits telephony-service configuration mode.

### Step 11
**Command or Action:**
```
ephone-dn dn-tag
```
**Example:**
```
Router(config)# ephone-dn 55
```
**Purpose:** Enters ephone-dn configuration mode to define an ephone-dn to receive night-service treatment.
- *dn-tag*—Unique sequence number that identifies the ephone-dn to receive night-service treatment.

### Step 12
**Command or Action:**
```
night-service bell
```
**Example:**
```
Router(config-ephone-dn)# night-service bell
```
**Purpose:** Marks this ephone-dn for night-service treatment. Incoming calls to this ephone-dn during the night-service time period send an alert notification to all IP phones that are marked to receive night-service bell notification.
Verifying Night Service

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 13 exit</td>
<td>Exits ephone-dn configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-ephone-dn)# exit</td>
<td></td>
</tr>
<tr>
<td>Step 14 ephone phone-tag</td>
<td>Enters ephone configuration mode. This is a phone that will be notified when an incoming call is received by a night-service ephone-dn during a night-service period.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# ephone 12</td>
<td></td>
</tr>
<tr>
<td>Step 15 night-service bell</td>
<td>Marks this phone to receive night-service bell notification when incoming calls are received on ephone-dns marked for night service during the night-service time period. The alert notification is a splash ring that is not associated with any of the individual lines on the IP phone and a visual display of the ephone-dn line number. The phone user can pick up the call by executing a PickUp or GPickUp.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-ephone)# night-service bell</td>
<td></td>
</tr>
</tbody>
</table>

Verifying Night Service

**Step 1** Use the `show running-config` command to verify the night-service parameters, which are listed in the telephony-service portion of the output, or use the `show telephony-service` command to display the same parameters.

Router# `show running-config`

telephony-service
   fxo hook-flash
   load 7910 P00403020214
   load 7960-7940 P00303020214
   max-ephones 48
   max-dn 288
   ip source-address 50.50.50.1 port 2000
   application segway0
   caller-id block code *321
   create cnf-files version-stamp 7960 Mar 07 2003 11:19:18
   voicemail 79000
   max-conferences 8
   call-forward pattern ..... 
   moh minuet.wav
   date-format yy-mm-dd
   transfer-system full-consult
   transfer-pattern ..... 
   secondary-dialtone 9
   night-service code *1234
   night-service day Tue 00:00 23:00
   night-service day Wed 01:00 23:59
   !
   !
Router# `show telephony-service`

CONFIG (Version=4.0(0))

Cisco Unified CallManager Express

---

**Cisco Unified CallManager Express System Administrator Guide**
Night Service

For on-line documentation please see:

ip source-address 10.103.3.201 port 2000
load 7910 P00403020214
load 7961 TERM41.7-0-1-1
load 7961GE TERM41.7-0-1-1
load 7960-7940 P00307020300
max-ephones 100
max-dn 500
max-conferences 8 gain -6
dspfarm units 2
dspfarm transcode sessions 4
dspfarm 1 MTP00059a3d7441
dspfarm 2
hunt-group report delay 1 hours
Number of hunt-group configured: 14
hunt-group logout DND
max-redirect 20
voicemail 7189
cnf-file location: system:
cnf-file option: PER-PHONE-TYPE
network-locale[0] US (This is the default network locale for this box)
user-locale[0] US (This is the default user locale for this box)
moh flash:music-on-hold.au
time-format 12
date-format mm-dd-yy
timezone 0 Greenwich Standard Time
secondary-dialtone 9
call-forward pattern .T
transfer-pattern 92.......
transfer-pattern 91........
transfer-pattern .T
after-hours block pattern 1 91900 7-24
after-hours block pattern 2 9976 7-24
after-hours block pattern 4 91...976.... 7-24
night-service date Jan 1 00:00 23:59
night-service day Mon 17:00 07:00
night-service day Wed 17:00 07:00
keepalive 30
timeout interdigit 10
timeout busy 10
timeout ringing 100
caller-id name-only: enable
system message XYZ Company
web admin system name xyz password xxxx
web admin customer name Customer
edit DN through Web: enabled.
edit TIME through web: enabled.
Log (table parameters):
   max-size: 150
   retain-timer: 15
create cnf-files version-stamp Jan 01 2002 00:00:00
transfer-system full-consult
multicast moh 239.10.10.1 port 2000
fxo hook-flash
local directory service: enabled.
Step 2  Use the `show running-config` command to verify that the correct ephone-dns and ephones are configured with the `night-service bell` command. You can also use the `show telephony-service ephone-dn` and `show telephony-service ephone` commands to display these parameters.

```
Router# show running-config

ephone-dn 24 dual-line
  number 2548
description FrontDesk
night-service bell

ephone 1
  mac-address 110F.80C0.FE0B
  type 7960 addon 1 7914
  no dnd feature-ring
  keep-conference
  button 1f40 2f41 3f42 4:30
  button 7m20 8m21 9m22 10m23
  button 11m24 12m25 13m26
night-service bell
```

Examples

The following example provides night service before 8 a.m. and after 5 p.m. Monday through Friday, before 8 a.m. and after 1 p.m. on Saturday, and all day Sunday. Extension 1000 is designated as a night-service extension. Incoming calls to extension 1000 during the night-service period ring on extension 1000 and provide night-service notification to phones that are designated as night-service phones. In this example, the night-service phones are ephone 14 and ephone 15. The night-service notification consists of a single ring on the phone and a display of “Night Service 1000.” A night-service toggle code has been configured, *6483 (*NITE), by which a phone user can activate or deactivate night-service conditions during the hours of night service.

```
telephony-service
  night-service day mon 17:00 08:00
  night-service day tue 17:00 08:00
  night-service day wed 17:00 08:00
  night-service day thu 17:00 08:00
  night-service day fri 17:00 08:00
  night-service day sat 13:00 12:00
  night-service day sun 12:00 08:00
  night-service code *6483
!
ephone-dn 1
  number 1000
  night-service bell
!
ephone-dn 2
  number 1001
  night-service bell
!
ephone-dn 10
  number 2222
!
ephone-dn 11
  number 3333
!
```
Troubleshooting Night-Service

Step 1 Use the **debug ephone** commands to observe messages and states associated with an ephone. For more information, see the *Cisco IOS Debug Command Reference*.

Feature History for Night Service

<table>
<thead>
<tr>
<th>Cisco Unified CME Version</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.0</td>
<td>Night service was introduced.</td>
</tr>
<tr>
<td>3.3</td>
<td>The behavior of the night-service code was changed. Previously, using the night-service code at a phone either enabled or disabled night service for the ephone-dns on that phone. Now, using the night-service code at a phone enables or disables night service for all night-service ephone-dns.</td>
</tr>
<tr>
<td>4.0</td>
<td>The <strong>night-service everyday</strong>, <strong>night-service weekday</strong>, and <strong>night-service weekend</strong> commands were introduced.</td>
</tr>
</tbody>
</table>

Related Features

**Automatic Call Forwarding During Night-Service**
To have an ephone-dn forward all its calls automatically during night-service hours, use the **call-forward night-service** command. For more information, see the “Call Forwarding” section on page 372.

**Ephone Templates**
The **night-service bell** command specifies that a phone will receive night-service notification when calls are received at ephone-dns that are configured as night-service ephone-dns. This command can be included in an ephone template that is applied to one or more individual ephones.

For more information, see the “Ephone Templates” section on page 318.
Overlaid Ephone-dns

Overlaid ephone-dns are ephone-dns that share the same physical line button on an IP phone. Overlaid ephone-dns can be used to receive incoming calls and place outgoing calls. Up to 25 ephone-dns can be assigned to a single phone button. This section discusses the following topics:

- Overlaid Ephone-dns Overview, page 429
- Restrictions, page 432
- Configuring Overlaid Ephone-dns, page 432
- Verifying Overlaid Ephone-dns, page 434
- Examples, page 435
- Troubleshooting Overlaid Ephone-dns, page 440
- Feature History for Overlaid Ephone-dns, page 440
- Related Features, page 441

Overlaid Ephone-dns Overview

Note

For a summary of the functionality introduced in different releases, see the “Feature History for Overlaid Ephone-dns” section on page 440.

Overlaid ephone-dns are a set of ephone-dns that occupy a single button on a phone. This section discusses the following topics:

- Overlaid Ephone-dns Basics, page 429
- Call Waiting for Overlaid Ephone-dns, page 430
- Extending Calls for Overlaid Ephone-dns to Other Buttons on the Same Phone, page 432

Overlaid Ephone-dns Basics

Overlaid ephone-dns are ephone-dns that share the same button on a phone. They can have the same extension number or different numbers. The same ephone-dns can appear on more than one phone and more than one phone can have the same set of overlaid ephone-dns.

The order in which overlaid ephone-dns are used by incoming calls can be determined by the call hunt commands, preference and huntstop. For example, ephone-dn 1 through ephone-dn 4 have the same extension number, 1001. Three phones are configured with the button 1o1,2,3,4 command. A call to 1001 will ring on the ephone-dn with the highest preference and display the caller ID on all phones that are on hook. If another incoming call to 1001 is placed while the first call is active (and the first ephone-dn with the highest preference is configured with the no huntstop command), the second call will roll over to the ephone-dn with the next-highest preference, and so forth. For more information, see the “Call Hunt” section on page 379.

If the ephone-dns in an ephone-dn overlay use different numbers, incoming calls will go to the ephone-dns with highest preferences. If no preferences are configured, the dial-peer hunt command setting will be used to determine which ephone-dns are used for incoming calls. The default setting for the dial-peer hunt command is to randomly select an ephone-dn that matches the called number.
To continue or to stop the search for ephone-dns, you must use, respectively, the no huntstop and huntstop commands under the individual ephone-dns. The huntstop setting is applied only to the dial peers affected by the ephone-dn command in telephony-service mode. Dial peers configured in global configuration mode comply with the global configuration huntstop setting.

When a call is answered by an ephone-dn, that ephone-dn is no longer accessible to other phones that share the ephone-dn in overlay mode. For example, if extension 1001 is answered by phone 1, caller ID for extension 1001 remains on phone 1 and is removed from the displays of phone 2 through phone 3. All actions pertaining to the call to extension 1001 (ephone-dn 1) are visible from the phone 1 display only. If phone 1 puts extension 1001 on hold, the other phones will not be able to directly pick up the on-hold call using a simple shared-line pickup. In addition, none of the other four phones will be able to make outgoing calls from the ephone-dn while it is in use. When they press the button 1, they will be connected to the next available ephone-dn listed in the button command. For example, if phone 1 and phone 2 are using ephone-dn 1 and ephone-dn 2, respectively, phone 3 would pick up ephone-dn 3 for an outgoing call.

If there are more phones than ephone-dns associated with an ephone-dn overlay set, it is possible for some phones to find that all the ephone-dns within their overlay set are in use by other phones. For example, if five phones have a line button configured with the button 1o1, 2, 3 command, there may be times when all three of the ephone-dns in the overlay set are in use. When that occurs, the other two phones will not be able to use an ephone-dn in the overlay set. When all ephone-dns in an overlay set are in use, phones with this overlay set will display the remote-line-in-use icon (a picture of a phone with a flashing X through it) for the corresponding line button. When at least one ephone-dn becomes available within the overlay set (that is, an ephone-dn is either idle or ringing), the phone display reverts to showing the status of the available ephone-dn (idle or ringing).

Dual-line ephone-dns can also use overlays. The configuration parameters are the same as for single-line ephone-dns, except that the huntstop channel command must be used to keep calls from hunting to the ephone-dn’s second channel.

Call Waiting for Overlaid Ephone-dns

Call waiting allows phone users to know that another person is calling them while they are talking on the phone. Phone users hear a call-waiting tone indicating that another party is trying to reach them. Calls to IP phones with soft keys can be answered with the Answer soft key. Calls to analog phones are answered using hookflash. When phone users answer a call-waiting call, their original call is automatically put on hold. If phone users ignore a call-waiting call, the caller is forwarded if call-forward no-answer has been configured.

For Cisco CME 3.2.1 and later versions, call waiting is available for overlaid ephone-dns. The difference in configuration between overlaid ephone-dns with call waiting and overlaid ephone-dns without call waiting is that overlaid ephone-dns with call waiting use the c keyword in the button command and overlaid ephone-dns without call waiting use the o keyword.

The behavior of overlaid ephone-dns with call waiting and overlaid ephone-dns without call waiting is the same, except for the following:

- Calls to numbers included in overlaid ephone-dns with call waiting will cause inactive phones to ring and active phones connected to other parties to generate auditory call-waiting notification. The default sound is beeping, but you can configure an ephone-dn to use a ringing sound. (See the “Call-Waiting Ring” section on page 392.) Visual call-waiting notification includes the blinking of handset indicator lights and the display of caller IDs.
For example, if three of four phones are engaged in calls to numbers from the same overlaid ephone-dn with call-waiting and another call comes in, the one inactive phone will ring, and the three active phones will issue auditory and visual call-waiting notification.

- In Cisco Unified CME 4.0 and later versions, up to six waiting calls can be displayed on Cisco Unified IP Phone 7940G, 7941G, 7941G-GE, 7960G, 7961G, 7961G-GE, 7970G, and 7971G-GE. For all other phones and earlier Cisco CME versions, two calls to numbers in an overlaid ephone-dn set can be announced. Subsequent calls must wait in line until one of the two original calls has ended. The callers who are waiting in the line will hear a ringback tone.

For example, a Cisco Unified IP Phone 7910 (maximum two call-waiting calls) has a button configured with a set of overlaid ephone-dns with call waiting (button 1c1,2,3,4). A call to ephone-dn 1 is answered. A call to ephone-dn 2 comes in and call-waiting notification is issued. Calls to ephone-dn 3 and ephone-dn 4 will wait in line and remain invisible to the phone user until one of the two original calls ends. When the call to ephone-dn 1 ends, the phone user will then talk to the person who called ephone-dn 2. The call to ephone-dn 3 will issue call-waiting notification while the call to ephone-dn 4 waits in line. (If the phone was a Cisco Unified IP Phone 7960, six calls could be waiting.)

Note that if an overlaid ephone-dn has call-forward-no-answer configured, calls to the ephone-dn that are unanswered before the no-answer timeout expires are forwarded to the destination that has been configured. If call-forward-no-answer is not configured, incoming calls receive ringback tones until the calls are answered.

More than one phone can use the same set of overlaid ephone-dns. In this case, the behavior is slightly different. The following example demonstrates call waiting for overlaid ephone-dns that are shared on two phones.

ephone 1
button 1c1,2,3,4
ephone 2
button 1c1,2,3,4

1. A call to ephone-dn 1 rings on ephone 1 and on ephone 2. Ephone 1 answers, and the call is no longer visible to ephone 2.
2. A call to ephone-dn 2 issues a call-waiting notification to ephone 1 and rings on ephone 2, which answers. The second call is no longer visible to ephone 1.
3. A call to ephone-dn 3 issues a call-waiting notification to ephone 1 and ephone 2. Ephone 1 puts the call to ephone-dn 1 on hold and answers the call to ephone-dn 3. The call to ephone-dn 3 is no longer visible to ephone 2.
4. A call to ephone-dn 4 is issues a call-waiting notification on ephone 2. The call is not visible on ephone 1 because it has met the two-call maximum by handling the calls to ephone-dn 1 and ephone-dn 3. (Note that the call maximum is six for those phones that are able to handle six call-waiting calls, as previously described.)

Phones configured for call waiting will not generate call-waiting notification when they are transferring calls or hosting conference calls.

Note

Ephone-dns accept call interruptions, such as call waiting, by default. For call waiting to work, the default must be active. To ensure that this is the case, remove the no call-waiting beep accept command from the configurations of ephone-dns for which you want to use call waiting. For more information, refer to the Cisco Unified CallManager Express Command Reference.
Extending Calls for Overlaid Ephone-dns to Other Buttons on the Same Phone

Phones with overlaid ephone-dns can use the `button` command with the `x` keyword to dedicate one or more additional buttons to receive overflow calls. If an overlay button is busy, an incoming call to any of the other ephone-dns in the overlay set rings on the first available overflow button on each phone that has been configured to receive the overflow. This feature works only with overlaid ephone-dns that are configured using the `button` command and the `o` keyword and not with overlaid ephone-dns that are configured using the `button` command and the `c` keyword or other types of ephone-dns that are not overlaid.

The comparison is that when you use the `button` command and the `c` keyword, it results in multiple calls on one button (the button is overlaid with multiple ephone-dns that have call waiting), and when you use the `button` command with the `o` keyword and the `x` keyword, it results in one call per button, but calls on multiple buttons.

For example, an ephone has an overlay button with ten numbers assigned to it using the `button` command and the `o` keyword. The next two buttons on the phone are configured using the `button` command and the `x` keyword. These buttons are reserved to receive additional calls to the overlaid extensions on the first button when the first button is in use.

```plaintext
ephone 276
button 1o24,25,26,27,28,29,30,31,32,33 2x1 3x1
```

Restrictions

- Call waiting is disabled when you configure ephone-dn overlays using the `button` command and the `o` keyword. To enable call waiting, you must configure ephone-dn overlays using the `button` command and the `c` keyword.
- The feature that allows rollover of overlay calls to another phone button using the `x` keyword only works to expand coverage for an overlay button that has been configured using the `o` keyword in the `button` command. Overlay buttons with call waiting that use the `c` keyword in the `button` command are not eligible for overlay rollover.

Configuring Overlaid Ephone-dns

This procedure assigns multiple ephone-dns to a single phone button and may also assign call waiting or dedicate overflow buttons.

SUMMARY STEPS

1. enable
2. configure terminal
3. ephone-dn phone-tag [dual-line]
4. number number
5. preference preference-value
6. no huntstop
7. huntstop channel
8. exit
9. ephone phone-tag
10. **mac-address** mac-address

11. **button** button-number\{(o | c)dn-tag, dn-tag[, dn-tag...]\} button-number\{x\} overlay-button-number

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router&gt; enable</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router# configure terminal</td>
</tr>
<tr>
<td><strong>Step 3</strong> ephone-dn phone-tag dual-line</td>
<td>Enters ephone-dn configuration mode to create an extension (ephone-dn) for a Cisco Unified IP phone line.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config)# ephone-dn 10 dual-line</td>
</tr>
<tr>
<td><strong>Step 4</strong> number number</td>
<td>Associates a telephone or extension number with an ephone-dn.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-ephone-dn)# number 1001</td>
</tr>
<tr>
<td><strong>Step 5</strong> preference preference-order</td>
<td>Sets dial-peer preference order for an ephone-dn.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-ephone-dn)# preference 1</td>
</tr>
<tr>
<td><strong>Step 6</strong> no huntstop</td>
<td>Continues call hunting behavior for an ephone-dn.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-ephone-dn)# no huntstop</td>
</tr>
<tr>
<td><strong>Step 7</strong> huntstop channel</td>
<td>(Recommended for dual-line ephone-dns) Keeps incoming calls from hunting to the second channel if the first channel is busy or does not answer.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-ephone-dn)# huntstop channel</td>
</tr>
<tr>
<td><strong>Step 8</strong> exit</td>
<td>Exits ephone-dn configuration mode</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-ephone-dn)# exit</td>
</tr>
</tbody>
</table>
Verifying Overlaid Ephone-dns

Step 1 Use the `show running-config` command or the `show telephony-service ephone` command to view button assignments.

```
Router# show running-config

ephone 5
description Cashier1
mac-address 0117.FBC6.1985
type 7960
button 1o4,5,6,200,201,202,203,204,205,206 2x1 3x1
```
Examples

This section contains the following examples:

- Overlaid Ephone-dn: Example, page 435
- Overlaid Dual-Line Ephone-dn: Example, page 435
- Overlaid Ephone-dn with Call Waiting: Example, page 436
- Overlaid Ephone-dns with Rollover Buttons: Example, page 437
- Called Directory Name Display for Overlaid Ephone-dns: Example, page 438
- Called Ephone-dn Name Display for Overlaid Ephone-dns: Example, page 439

Overlaid Ephone-dn: Example

The following example creates three lines (ephone-dns) that are shared across three IP phones to handle three simultaneous calls to the same telephone number. Three instances of a shared line with the extension number 1001 are overlaid onto a single button on each of three phones. A typical call flow is as follows. The first call goes to ephone 1 (highest preference) and rings button 1 on all three phones (huntstop is off). The call is answered on ephone 1. A second call to extension 1001 hunts onto ephone-dn 2 and rings on the two remaining phones, 11 and 12. The second call is answered by ephone 12. A third simultaneous call to extension 1001 hunts onto ephone-dn 3 and rings on ephone 11, where it is answered. Note that the no huntstop command is used to allow hunting for the first two ephone-dns, and the huntstop command is used on the final ephone-dn to stop call-hunting behavior. The preference command is used to create different selection preferences for each ephone-dn.

ephone-dn 1
  number 1001
  no huntstop
  preference 0

ephone-dn 2
  number 1001
  no huntstop
  preference 1

ephone-dn 3
  number 1001
  huntstop
  preference 2

ephone 10
  button 101,2,3

ephone 11
  button 101,2,3

ephone 12
  button 101,2,3

Overlaid Dual-Line Ephone-dn: Example

The following example shows how to overlay dual-line ephone-dns. In addition to using the huntstop and preference commands, you must use the huntstop channel command to prevent calls from hunting to the second channel of an ephone-dn. This example overlays five ephone-dns on button 1 on five different ephones. This allows five separate calls to the same number to be connected simultaneously, while occupying only one button on each phone.

ephone-dn 10 dual-line
Overlaid Ephone-dn with Call Waiting: Example

In following example, button 1 on ephone 1 though ephone 3 uses the same set of overlaid ephone-dns with call waiting that share the number 1111. The button also accept calls to each ephone’s unique (nonshared) ephone-dn number. Note that if ephone-dn 10 and ephone-dn 11 are busy, the call will go to ephone-dn 12. If ephone-dn 12 is busy, the call will go to voice mail.

ephone-dn 1 dual-line
number 1001

ephone-dn 2 dual-line
number 1001

ephone-dn 3 dual-line
number 1001
ephone-dn 10 dual-line
  number 1111
  no huntstop
  huntstop channel
call-forward noans 7000 timeout 30
ephone-dn 11 dual-line
  number 1111
  preference 1
  no huntstop
  huntstop channel
call-forward noans 7000 timeout 30
ephone-dn 12 dual-line
  number 1111
  preference 2
  huntstop channel
call-forward noans 7000 timeout 30
call-forward busy 7000
ephone 1
  button 1c1,10,11,12
ephone 2
  button 1c2,10,11,12
ephone 3
  button 1c3,10,11,12

Overlaid Ephone-dns with Rollover Buttons: Example

The following example configures a “3x3” shared-line setup for three phones and nine shared lines (ephone-dns 20 through 28). Each ephone has a unique ephone-dn for each of its three buttons (ephone-dns 11 through 13 on ephone 1, ephone-dns 14 through 16 on ephone 2, and ephone-dns 17 through 19 on ephone 3). The rest of the ephone-dns are shared among the three phones. Three phones with three buttons each can take nine calls. The overflow buttons provide the ability for an incoming call to ring on the first available button on each phone.

ephone-dn 11
  number 2011
ephone-dn 12
  number 2012
ephone-dn 13
  number 2013
ephone-dn 14
  number 2014
  .
  .
ephone-dn 28
  number 2028
ephone 1
  button 1o11,12,13,20,21,22,23,24,25,26,27,28 2x1 3x1
ephone 2
  button 1o14,15,16,20,21,22,23,24,25,26,27,28 2x1 3x1
Overlaid Ephone-dns

Called Directory Name Display for Overlaid Ephone-dns: Example

The following example demonstrates the display of a directory name for a called ephone-dn that is part of an overlaid ephone-dn set. For configuration information, see the “Called-Name Display” section on page 537.

This configuration of overlaid ephone-dns uses wildcards in the secondary numbers for the ephone-dns. The wildcards allow you to control the display according to the number that was dialed. The example is for a medical answering service with three IP phones that accept calls for nine doctors on one button. When a call to 5550001 rings on button 1 on ephone 1 through ephone 3, “doctor1” is displayed on all three ephones.

telephony-service
  service dnis dir-lookup

  directory entry 1 5550001 name doctor1
  directory entry 2 5550002 name doctor2
  directory entry 3 5550003 name doctor3

  directory entry 4 5550010 name doctor4
  directory entry 5 5550011 name doctor5
  directory entry 6 5550012 name doctor6

  directory entry 7 5550020 name doctor7
  directory entry 8 5550021 name doctor8
  directory entry 9 5550022 name doctor9

  ephone-dn 1
    number 5500 secondary 555000.

  ephone-dn 2
    number 5501 secondary 555001.

  ephone-dn 3
    number 5502 secondary 555002.

  ephone 1
    button 1,2,3
    mac-address 1111.1111.1111

  ephone 2
    button 1,2,3
    mac-address 2222.2222.2222

  ephone 3
    button 1,2,3
    mac-address 3333.3333.3333

The following example shows a hunt-group configuration for a medical answering service with two phones and four doctors. Each phone has two buttons, and each button is assigned two doctors’ numbers. When a patient calls 5550341, Cisco Unified CME matches the hunt-group pilot secondary number (555....), rings button 1 on one of the two phones, and displays “doctor1.” For more information about hunt-group behavior, refer to the “Ephone Hunt Groups” section on page 396. Note that wildcards are used only in secondary numbers and cannot be used with primary numbers.

telephony-service
  service dnis dir-lookup
  max-redirect 20
Called Ephone-dn Name Display for Overlaid Ephone-dns: Example

The following example demonstrates the display of the name assigned to the called ephone-dn using the `name` command. For information about configuring this feature, see the “Called-Name Display” section on page 537.

In this example, three phones have button 1 assigned to pick up three shared 800 numbers for three different catalogs.

The default display for the phones is the number of the first ephone-dn listed in the overlay set (18005550000). A call is made to the first ephone-dn (18005550000), and the caller ID (for example, 4085550123) is visible on all phones. The user for phone 1 answers the call. The caller ID (4085550123) remains visible on phone 1, and the displays on phone 2 and phone 3 return to the default display (18005550000). A call to the second ephone-dn (18005550001) is made. The default display on phone 2 and phone 3 is replaced with the called ephone-dn's name (catalog1) and number (18005550001).
Troubleshooting Overlaid Ephone-dns

**Step 1** Use the `show ephone overlay` command to display the configuration and current status of registered overlay ephone-dns.

```
Router# show ephone overlay
ephone-1 Mac:0007.0EA6.353A TCP socket:[1] activeLine:0 REGISTERED
mediaActive:0 offhook:0 ringing:0 reset:0 reset_sent:0 paging 0 debug:0
IP:10.2.225.205 52486 Telecaster 7960 keepalive 2771 max_line 6
button 1: dn 11 number 60011 CH1 IDLE overlay
button 2: dn 17 number 60017 CH1 IDLE overlay
button 3: dn 24 number 60024 CH1 IDLE overlay
button 4: dn 30 number 60030 CH1 IDLE overlay
button 5: dn 36 number 60036 CH1 IDLE CH2 IDLE overlay
button 6: dn 39 number 60039 CH1 IDLE CH2 IDLE overlay
overlay 1: 11(60011) 12(60012) 13(60013) 14(60014) 15(60015) 16(60016)
overlay 2: 17(60017) 18(60018) 19(60019) 20(60020) 21(60021) 22(60022)
overlay 3: 23(60023) 24(60024) 25(60025) 26(60026) 27(60027) 28(60028)
overlay 4: 29(60029) 30(60030) 31(60031) 32(60032) 33(60033) 34(60034)
overlay 5: 35(60035) 36(60036) 37(60037)
overlay 6: 38(60038) 39(60039) 40(60040)
```

**Step 2** Use the `show dialplan number` command to display all the number resolutions of a particular phone number, which allows you to detect whether calls are going to unexpected destinations. This command is useful for troubleshooting cases in which you dial a number but the expected phone does not ring.

Feature History for Overlaid Ephone-dns

<table>
<thead>
<tr>
<th>Cisco Unified CME Version</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.0</td>
<td>Overlaid ephone-dns were introduced and the o keyword was added to the button command.</td>
</tr>
</tbody>
</table>
## Related Features

### Called-Name Display

This feature allows you to specify that the name of the called party, rather than the number, should be displayed for incoming calls. This feature is very helpful for agents answering calls for multiple ephone-dns that appear on a single line button in an ephone-dn overlay set. For more information, see the “Called-Name Display” section on page 537.

### Ephone-dns

For a discussion of different types of ephone-dns, see the “Cisco Unified CallManager Express Overview” section on page 21.

---

<table>
<thead>
<tr>
<th>Cisco Unified CME Version</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.2.1</td>
<td>Call waiting for overlaid ephone-dns was introduced and the c keyword was added to the button command.</td>
</tr>
</tbody>
</table>
| 4.0                      | • The number of ephone-dns that can be overlaid on a single button using the button command and the o or c keyword was increased from 10 to 25.  
• The ability to extend calls for overlaid ephone-dns to other buttons (rollover buttons) on the same phone was introduced. Rollover buttons are created by using the x keyword with the button command.  
• The number of waiting calls that can be displayed for overlaid ephone-dns that have call waiting configured has been increased to six for the following phone types: Cisco Unified IP Phone 7940G, 7941G, 7941G-GE, 7960G, 7961G, 7961G-GE, 7970G, and 7971G-GE. |
Call-Handling Features

This chapter describes the following features that affect the way you make or handle calls:

- Call Blocking Based on Date and Time (After-Hours Toll Bar), page 444
- Call Hold, page 450
- Call Park, page 454
- Call Transfer, page 465
- Caller ID Blocking, page 475
- Conferencing, page 480

\[Note\]

Prior to version 4.0, the name of this product was Cisco CallManager Express (Cisco CME). Prior to version 3.0, the name was Cisco IOS Telephony Services (Cisco ITS).

\[Note\]


Call-Handling Features Overview

The features in this section affect the way that you can make calls or manipulate existing calls. Table 30 summarizes these features.

\[Table 30\] Call-Handling Features Summary

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Benefit</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Call Blocking Based on Date and Time (After-Hours Toll Bar)</td>
<td>System does not allow calls to specified number patterns during specified time periods.</td>
<td>Phone users are unable to make unauthorized calls.</td>
<td>During business hours, phone users at a company can make international calls. On nights and weekends, these calls are not permitted from phones unless the phone is marked as exempt and the user logs in with a PIN.</td>
</tr>
</tbody>
</table>
### Call-Handling Features

#### Table 30  Call-Handling Features Summary

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Benefit</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Call Hold</td>
<td>System changes call state from connected to hold.</td>
<td>Phone user can temporarily hold a call while performing another activity.</td>
<td>The phone user at extension 435 presses the Hold soft key to ask a question of a coworker and later presses Hold again to retrieve the call.</td>
</tr>
<tr>
<td>Call Park</td>
<td>System changes call state from connected to hold on a different ephone-dn.</td>
<td>Phone users can place a call on hold on a special ephone-dn that is used as a temporary parking spot from which the call can be retrieved by anyone on the system.</td>
<td>The phone user at extension 435 presses the Park soft key and the call is parked at the call slot with extension number 135. Later, the phone user at extension 458 presses the Pickup soft key and 135 to retrieve the call.</td>
</tr>
<tr>
<td>Call Transfer</td>
<td>System changes the connection of a call from one destination to another.</td>
<td>Phone users can connect existing calls to other lines without having the callers hang up and redial.</td>
<td>A service manager is speaking to a customer and realizes he has a billing question, and is able to transfer the customer to the accounting department.</td>
</tr>
<tr>
<td>Caller ID Blocking</td>
<td>System prevents the display of caller information on outgoing calls.</td>
<td>System administrators can prevent the display of caller ID information for individual phones or dial peers, or they can provide a code by which users can prevent caller ID display on individual calls.</td>
<td>A phone user dials the caller ID blocking code before making an outgoing call and the caller information is not displayed on the called phone.</td>
</tr>
<tr>
<td>Conferencing</td>
<td>System connects three parties in a single conversation.</td>
<td>Phone users can have multi-party conversations.</td>
<td>Extension 345 and 346 are in conversation and need information from the party at extension 347, who is then joined to their call.</td>
</tr>
</tbody>
</table>

### Call Blocking Based on Date and Time (After-Hours Toll Bar)

This feature blocks outgoing calls to specific number patterns during specified time periods. It also provides an override for individual phones. This section contains the following topics:

- Call Blocking Based on Date and Time Overview, page 445
- Configuring Call Blocking Based on Date and Time, page 445
- Verifying Call Blocking Based on Date and Time, page 448
- Examples, page 449
- Troubleshooting Call Blocking Based on Date and Time, page 449
- Feature History for Call Blocking Based on Date and Time, page 450
- Related Features
Call Blocking Based on Date and Time Overview

Note

For a summary of the functionality introduced in different releases, see the “Feature History for Call Blocking Based on Date and Time” section on page 450.

Call blocking to prevent unauthorized use of phones is implemented by matching dialed numbers against a pattern of specified digits and matching the time against the time of day and day of week or date that has been specified for call blocking. Up to 32 patterns of digits can be specified. Call blocking is supported on IP phones only and not on analog foreign exchange station (FXS) phones.

When a user attempts to place a call to digits that match a pattern that has been specified for call blocking during a time period that has been defined for call blocking, a fast busy signal is played for approximately 10 seconds. The call is then terminated and the line is placed back in on-hook status.

Call blocking applies to all IP phones in a Cisco Unified CME system, although individual IP phones can be exempted from all call blocking.

Individual phone users can be allowed to override call blocking associated with designated time periods by entering personal identification numbers (PINs) that have been assigned to their phones. For IP phones that support soft keys, such as the Cisco Unified IP Phone 7940G and the Cisco Unified IP Phone 7960G, the call-blocking override feature allows individual phone users to override the call blocking that has been defined for designated time periods. The system administrator must first assign a personal identification number (PIN) to any phone that will be allowed to override call blocking.

Then, to override call blocking, the phone user presses the Login soft key on the phone and enters the PIN that is associated with the phone. Note that logging in to a phone with a PIN only allows the user to override call blocking that is associated with particular time periods. Blocking patterns that are created with the 7-24 keyword in the after-hours block pattern command are in effect 7 days a week, 24 hours a day, and they cannot be overridden by using a PIN.

When PINs are configured for call-blocking override, they are cleared at a specific time of day or after phones have been idle for a specific amount of time. The time of day and amount of time can be set by the system administrator, or the defaults can be accepted.

Restrictions

- Call blocking is supported on IP phones only and not on analog foreign exchange station (FXS) phones.
- Call blocking override is supported only on phones that support soft-key display.

Configuring Call Blocking Based on Date and Time

This procedure specifies dial patterns and time periods during which calls to those dial patterns will be blocked.

SUMMARY STEPS

1. enable
2. configure terminal
3. telephony-service
4. **after-hours block pattern** `tag pattern [7-24]`
5. **after-hours day** `day start-time stop-time`
6. **after-hours date** `month date start-time stop-time`
7. **login** `[timeout [minutes]] [clear time]`
8. **restart all**
9. **exit**
10. **ephone** `phone-tag`
11. **after-hour exempt**
12. **pin** `pin-number`
13. **exit**

## DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
  **Example:**  
  Router> enable |
| **Step 2** configure terminal | Enters global configuration mode.  
  **Example:**  
  Router# configure terminal |
| **Step 3** telephony-service | Enters telephony-service configuration mode.  
  **Example:**  
  Router(config)# telephony-service |
| **Step 4** after-hours block pattern `tag pattern [7-24]` | Defines a pattern of outgoing digits to be blocked. Up to 32 patterns can be defined, using individual commands.  
  **Example:**  
  Router(config-telephony)# after-hours block pattern 1 91900  
  - If the 7-24 keyword is specified, the pattern is always blocked, 7 days a week, 24 hours a day.  
  - If the 7-24 keyword is not specified, the pattern is blocked during the days and dates that are defined using the after-hours day and after-hours date commands. |
### Command or Action

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| 5    | after-hours day day start-time stop-time | Defines a recurring time period based on the day of the week during which calls are blocked to outgoing dial patterns that are defined using the `after-hours block pattern` command.  
- **day**—Day of the week abbreviation. The following are valid day abbreviations: **sun**, **mon**, **tue**, **wed**, **thu**, **fri**, **sat**.  
- **start-time stop-time**—Beginning and ending times for call blocking, in an HH:MM format using a 24-hour clock. If the stop time is a smaller value than the start time, the stop time occurs on the day following the start time. For example, “**mon 19:00 07:00**” means “from Monday at 7 p.m. until Tuesday at 7 a.m.” |
| 6    | after-hours date month date start-time stop-time | Defines a recurring time period based on month and date during which calls are blocked to outgoing dial patterns that are defined using the `after-hours block pattern` command.  
- **month**—Month abbreviation. The following are valid month abbreviations: **jan**, **feb**, **mar**, **apr**, **may**, **jun**, **jul**, **aug**, **sep**, **oct**, **nov**, **dec**.  
- **date**—Date of the month. Range is from 1 to 31.  
- **start-time stop-time**—Beginning and ending times for call blocking, in an HH:MM format using a 24-hour clock. The stop time must be larger than the start time. The value 24:00 is not valid. If 00:00 is entered as an stop time, it is changed to 23:59. If 00:00 is entered for both start time and stop time, calls are blocked for the entire 24-hour period on the specified date. |
| 7    | login [timeout [minutes]] [clear time] | Specifies that the Cisco Unified CME system should deactivate all user logins at a specific time or after a designated period of idle time on a phone.  
- **timeout**—(Optional) Deactivates logins a given number of minutes after a phone becomes idle.  
- **minutes**—(Optional) Number from 5 to 1440. Default is 60.  
- **clear**—(Optional) Deactivates all logins at a specified time.  
- **time**—(Optional) Time of day using 00:00 to 24:00 on a 24-hour clock. For example, 10:30 p.m. is 22:30. Default is 24:00 (midnight). |
| 8    | restart all | Performs a fast reboot of all phones associated with this Cisco Unified CME router. Does not contact the DHCP or TFTP server for updated information. |

**Example:**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>after-hours day day start-time stop-time</td>
<td>Router(config-telephony)# after-hours day mon 19:00 7:00</td>
</tr>
<tr>
<td>after-hours date month date start-time stop-time</td>
<td>Router(config-telephony)# after-hours date jan 1 0:00 0:00</td>
</tr>
<tr>
<td>login [timeout [minutes]] [clear time]</td>
<td>Router(config-telephony)# login timeout 120 clear 23:00</td>
</tr>
<tr>
<td>restart all</td>
<td>Router(config-telephony)# restart all</td>
</tr>
</tbody>
</table>
### Verifying Call Blocking Based on Date and Time

**Step 1**  Use the `show running-config` command to display an entire configuration, including call blocking number patterns and time periods and the phones that are marked as exempt from call blocking.

```
telephony-service
fxo hook-flash
load 7960-7940 p00305000600
load 7914 s00103020002
max-ephones 100
max-dn 500
ip source-address 10.115.43.121 port 2000
timeouts ringing 10
voicemail 7189
max-conferences 8 gain -6
moh music-on-hold.au
web admin system name sys3 password sys3
dn-webedit
time-webedit
transfer-system full-consult
transfer-pattern .T
secondary-dialtone 9
after-hours block pattern 1 91900 7-24
after-hours block pattern 2 9976 7-24
after-hours block pattern 3 9011 7-24
after-hours block pattern 4 91...976.... 7-24
!
create cnf-files version-stamp 7960 Jul 13 2004 03:39:28
```
Step 2 Use the `show telephony-service` command to display only the portions of the configuration that show the call-blocking number patterns and time periods, and the `show telephony-service ephone` command to display only the ephone configurations.

Examples

The following example defines several patterns of digits for which outgoing calls are blocked. Patterns 1 and 2, which block calls to external numbers that begin with “1” and “011,” are blocked on Monday through Friday before 7 a.m. and after 7 p.m., on Saturday before 7 a.m. and after 1 p.m., and all day Sunday. Pattern 3 blocks calls to 900 numbers 7 days a week, 24 hours a day. The IP phone with tag number 23 and MAC address 00e0.8646.9242 is not restricted from calling any of the blocked patterns.

```
telephony-service
  after-hours block pattern 1 91
  after-hours block pattern 2 9011
  after-hours block pattern 3 91900 7-24
  after-hours block day mon 19:00 07:00
  after-hours block day tue 19:00 07:00
  after-hours block day wed 19:00 07:00
  after-hours block day thu 19:00 07:00
  after-hours block day fri 19:00 07:00
  after-hours block day sat 13:00 12:00
  after-hours block day sun 12:00 07:00
!
ephone 23
  mac 00e0.8646.9242
  button 1:33
  after-hour exempt
!
ephone 24
  mac 2234.1543.6352
  button 1:34
```

The following example deactivates a phone’s login after three hours of idle time and clears all logins at 10 p.m.:

```
ephone 1
  pin 1000
!
telephony-service
  login timeout 180 clear 2200
```

Troubleshooting Call Blocking Based on Date and Time

Step 1 Use the `show ephone login` command to display the login status of all phones.

```
Router# show ephone login
ephone 1            Pin enabled:TRUE      Logged-in:FALSE
ephone 2            Pin enabled:FALSE
ephone 3            Pin enabled:FALSE
```
Feature History for Call Blocking Based on Date and Time

<table>
<thead>
<tr>
<th>Cisco Unified CME Version</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.0</td>
<td>Call blocking based on date and time was introduced. Override for call blocking was also introduced.</td>
</tr>
</tbody>
</table>

Related Features

Soft Key Control
To move or remove the Login soft key on one or more phones, create and apply an ephone template that contains the appropriate softkeys commands.
For more information, see the “Soft-Key Display” section on page 551.

Call Hold

Call hold allows you to place a call into the hold state so that you can answer a second call or perform another activity without disconnecting the existing call. This section describes the following topics:

- Call Hold Overview, page 450
- Configuring Call Hold, page 451
- Verifying Call Hold, page 452
- Examples, page 453
- Troubleshooting Call Hold, page 453
- Feature History for Call Hold, page 453
- Related Features, page 453

Call Hold Overview

For a summary of the functionality introduced in different releases, see the “Feature History for Call Hold” section on page 453.

On IP phones, you can place a call on hold by pressing the Hold soft key or the Hold button, depending on the type of phone you have. To retrieve the call, press Hold again.

On analog phones, you press a Flash key or use hookflash to place a call on hold. To retrieve the call, press Flash or hookflash again.

On a single-line ephone-dn, if you want to use call hold with multiple-line features like call waiting, call transfer, and conferencing, you must have an additional, available ephone-dn on the same phone. Dual-line ephone-dns have an extra channel available to handle these multiple-line features without requiring additional lines.
On-hold notification is an optional feature that generates a ring burst on idle IP phones that have placed a call on hold. An option is available to generate call-waiting beeps for occupied phones that have placed calls on hold. This feature is disabled by default.

## Configuring Call Hold

Call hold is available by default and no configuration is required for the basic feature. You can, however, specify the generation of an audible alert to remind you that a call is waiting on hold.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ephone-dn dn-tag [dual-line]**
4. **hold-alert timeout {idle | originator | shared}**
5. **exit**

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router&gt; enable</td>
<td>Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> ephone-dn dn-tag [dual-line]</td>
<td>Enters ephone-dn configuration mode, creates an ephone-dn, and optionally assigns it dual-line status.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# ephone-dn 20</td>
<td>• <strong>dn-tag</strong>—Unique sequence number that identifies this ephone-dn during configuration tasks. The maximum number of ephone-dns for a particular Cisco Unified CME system is version- and platform-specific. Refer to CLI help for the range of values.</td>
</tr>
<tr>
<td></td>
<td>• <strong>dual-line</strong>—(Optional) Enables an ephone-dn with one voice port and two voice channels, which supports features such as call waiting, call transfer, and conferencing with a single ephone-dn.</td>
</tr>
</tbody>
</table>
Call-Handling Features

Verifying Call Hold

Step 1  Use the `show running-config` command to verify your configuration. On-hold call notification is listed in the ephone-dn portion of the output.

   `Router# show running-config`

   ephone-dn 1 dual-line
   number 126 secondary 1261
   call-forward busy 500
   call-forward noan 500 timeout 10
   hold-alert 15 idle

Step 2  Use the `show telephony-service ephone-dn` command to display on-hold call notification information.

   `Router# show telephony-service ephone-dn`

   ephone-dn 2
   number 5002
   hold-alert 15 idle
   call-forward noan 5001 timeout 8

Example:

   Router(config-ephone-dn)# hold-alert 15 idle

Sets audible alert notification on the Cisco Unified IP phone for alerting the user about on-hold calls.

- **Timeout**: Specifies the time interval from the time the call is placed on hold to the time the on-hold audible alert is generated, in seconds. The alert is repeated at the end of the set timeout value.

- **Idle**: Generates a one-second burst of ringing on the IP phone that placed the call in the hold state if that phone is in the idle state. If the phone is in active use, no on-hold alert is generated.

- **Originator**: Generates a one-second burst of ringing on the phone that placed the call into the hold state if the phone is in the idle state. If the phone is in use on another call, an audible beep is generated (call-waiting tone).

**Note**: From the perspective of the originator of the call on hold, the `originator` and `shared` keywords provide the same functionality.

- **Shared**: Generates a one-second burst of ringing for all the idle phones that share the same line appearance. If the phones are in use, they do not hear an audible beep, except for the phone that placed the call on hold, which does hear beeps.

Example:

   Router(config-ephone-dn)# exit

Exits ephone-dn configuration mode.
Examples

In the following example, extension 2555 is configured to not forward local calls that are internal to the Cisco Unified CME system. Extension 2222 dials extension 2555. If 2555 is busy, the caller hears a busy tone. If 2555 does not answer, the caller hears ringback. The internal call is not forwarded.

```plaintext
ephone-dn 25
  number 2555
  no forward local-calls
  call-forward busy 2244
  call-forward noan 2244 timeout 45
```

Troubleshooting Call Hold

**Step 1**  If you are not hearing call-waiting tones, use the `show telephony-service ephone-dn` command to verify the call-waiting parameters for the ephone-dn.

```plaintext
Router# show telephony-service ephone-dn
ephone-dn 3 dual-line
  number 126
  preference 2 secondary 9
  huntstop
  huntstop channel
  call-waiting beep
```

**Step 2**  Use the `debug ephone` commands to observe messages and states associated with an ephone. For more information, see the *Cisco IOS Debug Command Reference*.

Feature History for Call Hold

<table>
<thead>
<tr>
<th>Cisco Unified CME Version</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>Call hold was introduced.</td>
</tr>
<tr>
<td>2.0</td>
<td>On-hold notification was introduced.</td>
</tr>
</tbody>
</table>

Related Features

**Call Park**

You can use call park to place a call on hold at a special ephone-dn, called a call-park slot, from which other phone users can retrieve the call. See the “Call Park” section on page 454.
Call Park

The basic call park feature allows a phone user to place a call on hold on a special ephone-dn that is used as a temporary parking spot from which the call can be retrieved by anyone on the system. This section describes the following topics:

- Call Park Overview, page 454
- Configuring Call Park, page 458
- Verifying Call Park, page 462
- Examples, page 462
- Troubleshooting Call Park, page 464
- Feature History for Call Park, page 464
- Related Features, page 464

Call Park Overview

Note

For a summary of the functionality introduced in different releases, see the “Feature History for Call Park” section on page 464.

This section discusses the following topics:

- Basic Call Park, page 454
- Dedicated Call-Park Slots, page 456
- Call-Park Blocking, page 458
- Call-Park Redirect, page 458

Basic Call Park

Call park allows a phone user to place a call on hold at a special ephone-dn that is used as a temporary parking spot from which the call can be retrieved by anyone on the system. In contrast, a call that is placed on hold using the Hold button or Hold soft key can be retrieved only from the extension that placed the call on hold. The special ephone-dn at which a call is parked is known as a call-park slot. A call-park slot is a floating extension, or ephone-dn that is not bound to a physical phone, to which calls are sent to be held.

After at least one call-park slot has been defined and the Cisco Unified CME phones have been restarted, phone users are able to park calls using the Park soft key. Users who attempt to park a call at a busy slot hear a busy tone.

A caller who is parked in a park slot hears the music-on-hold (MOH) audio stream if the call uses the G.711 codec or if the call uses G.729 with transcoding, a feature that is available in Cisco CME 3.2 and later versions; otherwise, callers hear tone on hold.

A phone user who has parked a call can retrieve the call using the PickUp soft key and an asterisk (*). Phone users other than the one who parked the call can retrieve the call by pressing the PickUp soft key and the extension number of the call-park slot, which is available on their phone displays.
Directed call park allows calls to be transferred to a call-park-slot extension number using the Transfer key; a transfer to a call-park slot is always a blind transfer. Calls can also be forwarded from phones to call-park slot numbers. For versions prior to Cisco Unified CME 4.0, callers can directly dial call-park slot numbers to be placed in park. If another call is already parked in the slot, the caller hears a busy tone.

In Cisco Unified CME 4.0 and later versions, a direct call to a call-park slot is interpreted as an attempt to pick up a call that is parked there; if no call is parked in the slot, the caller hears a busy tone.

The ability to directly dial a park slot to retrieve a call is useful in the following scenario. An attendant connected to a remote Cisco Unified CME system can perform a directed call park (transfer-to-park) into a park slot on the local Cisco Unified CME router by simply transferring the call to the telephone number associated with the local Cisco Unified CME park slot. The remote attendant can then inform local phone users of the existence of the parked call by dialing (across VoIP) into a paging number on the local Cisco Unified CME system, or the parked call may simply be visible to one or more local users whose phones are configured to monitor the park-slot. Then, when a local IP phone user directly dials the extension number of the park slot, the system assumes that the user is requesting retrieval (pickup) of the call in the park slot. If there is no call in the park slot, the Cisco Unified CME system returns a busy tone to the local user.

A caller who is parked in a park slot hears the music-on-hold (MOH) audio stream if the call uses a G.711 codec or if it uses G.729 with transcoding, a feature that is available in Cisco CME 3.2 and later versions; otherwise, callers hear tone on hold.

Each call-park slot occupies one ephone-dn. During configuration, any number of ephone-dns can be designated as call-park slots using the `park-slot` command, as long as the total number of park slots and normal extensions does not exceed the maximum number of ephone-dns that was defined with the `max-dn` command. After an administrator defines at least one call-park slot and restarts phones, the Park soft key is displayed on all IP phones that are able to display soft keys.

Each call-park slot can hold one call at a time, so the number of simultaneous calls that can be parked is equal to the number of slots that have been created in the Cisco Unified CME system. In Cisco CME 3.2.1 and later releases, call-park slots can also be monitored. If a call-park slot is assigned to a monitor button using the `button m` command, the line status shows “in use” when a call is parked in the monitored slot. A call that is parked on the monitored call-park slot can be picked up by pressing the assigned monitor button.

You can create a call-park slot that is reserved for use by one extension by assigning that slot a number whose last two digits are the same as the last two digits of the extension. When an extension starts to park a call, the system searches first for a call-park slot that has the same final two digits as the extension. If no such call-park slot exists, the system chooses an available call-park slot.

Multiple call-park slots can be created with the same extension number so that more than one call can be parked for a particular department or group of people at a known extension number. For example, at a hardware store, calls for the plumbing department can be parked at extension 101, calls for lighting can be parked at 102, and so forth. Everyone in the plumbing department knows that calls parked at 101 are for them and can pick up calls from extension 101. When multiple calls are parked at the same call-park slot number, they are picked up in the order in which they were parked; that is, the call that has been parked the longest is the first call picked up from that call-park slot number.

For cases where multiple call-park slots use the same extension number, you must configure each ephone-dn that uses the extension number with the `no huntstop` command, except for the last ephone-dn to which calls are sent. In addition, each ephone-dn must be configured with the `preference` command. The preference numeric values must increase to match the order of the ephone-dns. That is, the lowest ephone-dn tag park-slot must have the lowest numeric preference number, and so forth. Without the configuration of the `preference` and `huntstop` commands, all calls that are parked after a second call has been parked will generate a busy signal. The caller who is being transferred to park will hear a busy signal, while the phone user who parked the call will receive no indication that the call was lost.
A reminder ring can be sent to the extension that parked the call by using the `timeout` keyword with the `park-slot` command. The `timeout` keyword and argument set the interval length during which the call-park reminder ring is timed out or inactive. If the `timeout` keyword is not used, no reminder ring is sent to the extension that parked the call. The number of timeout intervals and reminder rings are configured with the `limit` keyword and argument. For example, a limit of 3 timeout intervals sends 2 reminder rings (interval 1, ring 1, interval 2, ring 2, interval 3). The `timeout` and `limit` keywords and arguments also set the maximum time that calls stay parked. For example, a timeout interval of 10 seconds and a limit of 5 timeout intervals (park-slot timeout 10 limit 5) will park calls for approximately 50 seconds.

The reminder ring is sent only to the extension that parked the call unless the `notify` keyword is also used to specify an additional extension number to receive a reminder ring. When an additional extension number is specified using the `notify` keyword, the phone user at that extension can retrieve a call from this slot by pressing the PickUp soft key and the asterisk (*) key.

You can define the length of the timeout interval for calls parked at a call-park slot, as well as the number of timeout intervals that should occur before the call is either recalled or transferred. If you specify a transfer target in the `park-slot` command, the call is transferred to the specified target after the timeout intervals expire rather than to the primary number of the parking phone.

If a name has been specified for the call-park slot using the `name` command, that name will be displayed on a recall or transfer rather than an extension number.

You can also specify an alternate target extension to which to transfer a parked call if the recall or transfer target is in use. In use is defined as either ringing or connected. For example, a call is parked at the private park slot for the phone with the primary extension of 2001, as shown in Figure 36. After the timeouts expire, the system attempts to recall the call to extension 2001, but that line is connected to another call. The system then transfers the call to the alternate target, extension 3784.

**Dedicated Call-Park Slots**

A dedicated, private call-park slot can be configured for an ephone using the `reserved-for` keyword in the `park-slot` command. The dedicated call-park slot is associated with the primary extension of the ephone. All extensions on this phone can park calls in the dedicated park slot. The extensions on this phone are the only extensions that can park a call in the dedicated park slot. Only one call at a time can be parked in a park slot; a busy tone is returned to any attempt to park a call in a slot that is already in use.

Calls can be parked in dedicated call-park slots using any of the following methods (the extension doing the parking must be on a phone whose primary extension is associated with a dedicated park slot).

- With an active call, an IP phone user presses the Park soft key.
- With an active call, an IP phone user presses the Transfer soft key and a standard or custom FAC (feature access code) for the call-park feature. The standard FAC for call park is **6**.
- With an active call, an analog phone user presses hookflash and the standard or custom FAC for the call park feature.

Calls can be retrieved from dedicated call-park slots using any of the following methods:

- An IP phone user presses the Pickup soft key and dials the park-slot number.
- An IP phone user presses the New Call soft key and dials the park-slot number.
- An analog phone user lifts the handset, presses the standard or custom FAC for directed call pickup, and dials the park-slot number. The standard FAC for directed pickup is **5**.
If no dedicated park slot is found anywhere in the Cisco Unified CME system for an ephone-dn that is attempting to park a call, the system uses the standard call-park procedure; that is, the system searches for a preferred park slot (one with an ephone-dn number that matches the last two digits of the ephone-dn attempting to park the call) and if none is found, uses any available call-park slot.

Figure 36 shows an example of a dedicated call-park slot.

If the configuration specifies that a call should be recalled to the parking phone after the timeout intervals expire, the call is always returned to the phone’s primary extension number, regardless of which extension on the phone did the parking. Figure 36 shows an ephone that is configured with the extension numbers 2001, 2002, and 2003, and a private call-park slot at extension 3333. The private park slot has been set up to recall calls to the parking phone when the parked call’s timeouts expire. In the example, extension 2003 parks a call using the Park soft key. When the timeout intervals expire, the call rings back on extension 2001.

The configuration in Figure 36 specifies that the call will recall or transfer from the park slot after 3 times the 60-second timeout, or after 180 seconds. Also, prior to the exhaustion of the 3 timeouts the phone will receive reminder notifications that a parked call is waiting. The reminders are sent after each 60-second timeout interval expires (that is, at 60 seconds and at 120 seconds). You may want to set the timeout command with a limit of 1 instead, so that the call simply parks and recalls or transfers without sending a reminder ring.

**Figure 36  Dedicated Call Park Example**

<table>
<thead>
<tr>
<th>ephone-dn 1</th>
<th>number 2001</th>
</tr>
</thead>
<tbody>
<tr>
<td>ephone-dn 2</td>
<td>number 2002</td>
</tr>
<tr>
<td>ephone-dn 3</td>
<td>number 2003</td>
</tr>
<tr>
<td>ephone-dn 4</td>
<td>number 3333</td>
</tr>
</tbody>
</table>

name Park 2001
park-slot reserved-for 2001 timeout 60 limit 3 recall alternate 3754
ephone 2
button 1:1 2:2 3:3

1. A user on extension 2003 parks a call using the Park soft key.
2. After three intervals of 60 seconds, the call is recalled to the phone’s primary number, 2001.
3. If 2001 is busy, the call is transferred to 3754.
Call-Park Blocking

In Cisco Unified CME 4.0 and later versions, individual ephones can be prevented from making transfers to call-park slots by using the `transfer-park blocked` command. This command prevents transfers to park that use the Transfer soft key and a call-park slot number, while allowing call-parks that use only the Park soft key. (To prevent use of the Park soft key, use an ephone template to remove it from the phone. See the “Soft-Key Display” section on page 551).

An exception is made for phones with reserved, or dedicated, park slots. If the `transfer-park blocked` command is used on an ephone that has a dedicated park slot, the phone is blocked from parking calls at park slots other than the phone’s dedicated park slot but can still park calls at its own dedicated park slot.

Call-Park Redirect

By default, H.323 and SIP calls that use the call-park feature use hairpin call forwarding or transfer to park calls and to pick up calls from park. The `call-park system redirect` command allows you to specify that these calls should use H.450 or the SIP Refer method of call forwarding or transfer instead. The `no` form of the command returns the system to the default behavior.

Configuring Call Park

This procedure defines call-park slots and optional call-park blocking and call-park redirect.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `ephone-dn dn-tag [dual-line]`
4. `number number [secondary number] [no-reg [both | primary]]`
5. `park-slot [reserved-for extension-number] [timeout seconds limit count] [notify extension-number [only]] [recall] [transfer extension-number] [alternate extension-number] [retry seconds limit count]`
6. `exit`
7. `ephone phone-tag`
8. `transfer-park blocked`
9. `exit`
10. `telephony-service`
11. `call-park system redirect`
12. `restart all`
13. `exit`
## DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router&gt; enable</td>
<td>- Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> ephone-dn dn-tag [dual-line]</td>
<td>Enters ephone-dn configuration mode, creates an ephone-dn, and optionally assigns it dual-line status.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# ephone-dn 20</td>
<td>- <em>dn-tag</em>—Unique sequence number that identifies this ephone-dn during configuration tasks. The maximum number of ephone-dns for a particular Cisco Unified CME system is version- and platform-specific. Refer to CLI help for the range of values.</td>
</tr>
<tr>
<td></td>
<td>- <em>dual-line</em>—(Optional) Enables an ephone-dn with one voice port and two voice channels, which supports features such as call waiting, call transfer, and conferencing with a single ephone-dn.</td>
</tr>
<tr>
<td><strong>Step 4</strong> number number [secondary number] [no-reg [both</td>
<td>primary]]</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-ephone-dn)# number 2345</td>
<td>- <em>number</em>—String of up to 16 digits that represents a telephone or extension number to be associated with this ephone-dn.</td>
</tr>
<tr>
<td></td>
<td>- <em>secondary</em>—(Optional) Allows you to associate a second telephone number with an ephone-dn.</td>
</tr>
<tr>
<td></td>
<td>- <em>no-reg</em>—(Optional) Specifies that this number should not register with the H.323 gatekeeper. Unless you specify one of the optional keywords (both or primary) after the no-reg keyword, only the secondary number is not registered.</td>
</tr>
</tbody>
</table>
### Command or Action

<table>
<thead>
<tr>
<th>Step 5</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>park-slot</strong></td>
<td>[reserved-for extension-number] [timeout seconds limit count] [notify extension-number [only]] [recall] [transfer extension-number] [alternate extension-number] [retry seconds limit count]</td>
<td>Creates a floating extension (ephone-dn) at which calls can be temporarily held (parked).</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-ephone-dn)# park-slot reserved-for 2458 timeout 60 limit 3 recall alternate 3754</td>
<td></td>
</tr>
</tbody>
</table>

- **reserved-for extension-number**—(Optional) Indicates that this slot is a private park slot for the phone with the specified extension number as its primary line. All lines on that phone can use this park slot.
- **timeout seconds**—(Optional) Sets the call-park reminder timeout interval, in seconds. Range is from 0 to 65535. When the interval expires, the call-park reminder sends a 1-second ring and displays a message on the LCD panel of the Cisco Unified IP phone that parked the call and that of any extension that may be specified with the **notify** keyword. Default is that the reminder ring is sent only to the phone that parked the call.
- **limit count**—(Optional, applies to **timeout** keyword) Sets a limit for the number of time-out intervals for a parked call. For example, a limit of 3 sends 2 reminder rings (interval 1, ring 1, interval 2, ring 2, interval 3). A call parked at this slot is disconnected after the limit has been reached unless another action has been specified. Range is 1 to 65535.
- **notify extension-number**—(Optional) Sends a reminder ring to the specified extension in addition to the reminder ring that is sent to the phone that parked the call.
- **only**—(Optional) Sends a reminder ring only to the extension specified with the notify keyword and does not send a reminder ring to the phone that parked the call. This option allows all reminder rings for parked calls to be sent to a receptionist's phone or an attendant's phone, for example.
- **recall**—(Optional) Returns the call to the phone that parked it after the timeout limits expire.
- **transfer extension-number**—(Optional) Returns the call to the specified number after timeout limits expire.
- **alternate extension-number**—(Optional) Returns the call to the specified second target number if the recall or transfer target phone is in use on any of its extensions (ringing or in conversation).
- **retry seconds**—(Optional) Sets the delay before another attempt to recall or transfer a parked call, in seconds. Range is from 0 to 65535. Number of attempts is set by the **limit** keyword.
- **limit count**—(Optional, applies to **retry** keyword) Sets a limit for the number of retries. When a limit is set, a call parked at this slot is disconnected after the limit has been reached. Range is from 1 to 65535.
### Call-Handling Features

#### Call Park

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 6</strong> exit</td>
<td>Exits ephone-dn configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-ephone-dn)# exit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> ephone phone-tag</td>
<td>Enters ephone configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# ephone 25</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong> transfer-park blocked</td>
<td>(Optional) Prevents extensions on this ephone from transferring calls to call-park slots.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-ephone)# transfer-park blocked</td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong> telephony-service</td>
<td>Enters telephony-service configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# telephony-service</td>
<td></td>
</tr>
<tr>
<td><strong>Step 10</strong> call-park system redirect</td>
<td>Specifies that within the call-park feature, H.323 and SIP calls will use H.450 or the SIP Refer method of call forwarding or transfer to park calls and to pick up calls from park.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# call-park system redirect</td>
<td></td>
</tr>
<tr>
<td><strong>Step 11</strong> restart all</td>
<td>Performs a fast reboot of all phones associated with this Cisco Unified CME router. Does not contact the DHCP or TFTP server for updated information.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-telephony)# restart all</td>
<td></td>
</tr>
<tr>
<td><strong>Step 12</strong> exit</td>
<td>Exits telephony-service configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-telephony)# exit</td>
<td></td>
</tr>
</tbody>
</table>
Verifying Call Park

**Step 1** Use the `show running-config` command to verify your configuration. Call-park slots are listed in the `ephone-dn` portion of the output.

```
Router# show running-config

! ephone-dn 23
  number 853
  park-slot timeout 10 limit 1 recall
  description park slot for Sales
!
ephone-dn 24
  number 8126
  park-slot reserved-for 126 timeout 10 limit 1 transfer 8145
!
ephone-dn 25
  number 8121 secondary 121
  park-slot reserved-for 121 timeout 30 limit 1 transfer 8145
!
ephone-dn 26
  number 8136 secondary 136
  park-slot reserved-for 136 timeout 10 limit 1 recall
!
ephone-dn 30 dual-line
  number 451 secondary 501
  preference 10
  huntstop channel
!
ephone-dn 31 dual-line
  number 452 secondary 502
  preference 10
  huntstop channel
!
```

**Step 2** Use the `show telephony-service ephone-dn` command to display call park configuration information.

```
Router# show telephony-service ephone-dn

ephone-dn 26
  number 8136 secondary 136
  park-slot reserved-for 136 timeout 10 limit 1 recall
```

**Examples**

This section contains the following examples:

- Basic Call Park: Example, page 463
- Phone Blocked From Using Call Park: Example, page 463
- Call-Park Redirect: Example, page 463
Basic Call Park: Example
The following example creates a call-park slot with the number 1560. After a call is parked at this number, the system provides 10 reminder rings at intervals of 30 seconds to the extension that parked the call.

```plaintext
ephone-dn 50
   number 1560
   park-slot timeout 30 limit 10
```

Phone Blocked From Using Call Park: Example
The following example prevents ephone 25 and extensions 234, 235, and 236 from parking calls at any call-park slots.

```plaintext
ephone-dn 11
   number 234

ephone-dn 12
   number 235

ephone-dn 13
   number 236

ephone 25
   button 1:11 2:12 3:13
   transfer-park blocked
```

The following example sets up a dedicated park slot for the extensions on ephone 6 and blocks transfers to call park from extensions 2977, 2978, and 2979 on that phone. Those extensions can still park calls at the phone’s dedicated park slot by using the Park soft key or the Transfer soft key and the FAC for call park.

```plaintext
ephone-dn 3
   number 2558
   name Park 2977
   park-slot reserved-for 2977 timeout 60 limit 3 recall alternate 3754

ephone-dn 4
   number 2977

ephone-dn 5
   number 2978

ephone-dn 6
   number 2979

ephone 6
   button 1:4 2:5 3:6
   transfer-park blocked
```

Call-Park Redirect: Example
The following example specifies that H.323 and SIP calls that are parked should use H.450 or the SIP Refer method to when they are parked or picked up.

```plaintext
telephony-service
call-park system redirect
```
Troubleshooting Call Park

Step 1  Use the show ephone-dn park command to display configured call-park slots and their status, as shown in the following example:

Router# show ephone-dn park

DN 50 (1560) park-slot state IDLE
Notify to () timeout 30 limit 10

Step 2  Use the debug ephone commands to observe messages and states associated with an ephone. For more information, see the Cisco IOS Debug Command Reference.

Feature History for Call Park

<table>
<thead>
<tr>
<th>Cisco Unified CME Version</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1</td>
<td>Call park was introduced.</td>
</tr>
<tr>
<td>3.2.1</td>
<td>Monitoring of call-park slots was introduced.</td>
</tr>
<tr>
<td>4.0</td>
<td>Dedicated call-park slots, alternative recall locations, and call-park blocking were introduced. Direct calls to park slots are now interpreted as attempts to pick up parked calls rather than attempts to be parked at the slot.</td>
</tr>
</tbody>
</table>

Related Features

Ephone Templates

The transfer-park blocked command, which blocks transfers to call-park slots, can be included in ephone templates that are applied to individual ephones.

The Park soft key can be removed from the display of one or more phones by including the appropriate softkeys command in an ephone template and applying the template to individual ephones.

For more information, see the “Ephone Templates” section on page 318.

Feature Access Codes (FACs)

You can park calls using a feature access code (FAC) instead of a soft key on the phone if standard or custom FACs have been enabled for your system. The call-park FAC is considered a transfer to a call-park slot and therefore is valid only after the Transfer soft key (IP phones) or hookflash (analog phones) has been used to initiate a transfer. The following are the standard FACs for call park:

- Dedicated park slot—Standard FAC is **6.
- Any available park slot—Standard FAC is **6 plus optional park-slot number.

For more information about FACs, see the “Feature Access Codes” section on page 325.
Controlling Use of the Park Soft Key

To block the functioning of the call park (Park) soft key without removing the key display, create and apply an ephone template that contains the `features blocked` command. For more information, see the “Feature Control” section on page 329.

To remove the call park (Park) soft key from one or more phones, create and apply an ephone template that contains the appropriate `softkeys` command. For more information, see the “Soft-Key Display” section on page 551.

Call Transfer

When you are connected to another party, call transfer allows you to shift the connection of the other party to a different number. This section describes the following topics:

- Call Transfer Overview, page 465
- Configuring Call Transfer, page 467
- Verifying Call Transfer, page 472
- Examples, page 473
- Troubleshooting Call Transfer, page 474
- Feature History for Call Transfer, page 474
- Related Features, page 474

Call Transfer Overview

For a summary of the functionality introduced in different releases, see the “Feature History for Call Transfer” section on page 474.

Call transfer allows a phone user to connect a party on an existing call to another number. This section contains the following sections:

- Basic Call Transfer, page 465
- Consultative Transfer Support for Direct Station Select, page 466
- Call Transfer Blocking, page 467

Basic Call Transfer

Call transfer methods must be interoperable with the other networks with which you interface. Cisco CME 3.2 and later versions provide full call-transfer and call-forwarding interoperability with call processing systems on the network that support H.450.2, H.450.3, and H.450.12 standards. For call processing systems that do not support H.450 standards, Cisco CME 3.2 and later versions provide VoIP-to-VoIP hairpin call routing without requiring the use of the special Tool Command Language (Tcl) script that was needed in earlier releases of Cisco CME.

Call transfers can be blind or consultative. A blind transfer is one in which the transferring extension connects the caller to a destination extension before ringback begins. A consultative transfer is one in which the transferring party either connects the caller to a ringing phone (ringback heard) or speaks with the third party before connecting the caller to the third party.
Call-Handling Features

Call Transfer

Note
For a more complete discussion of network interoperability issues, see the “Transfer and Forwarding Support” section on page 223.

Cisco CME 3.0 and Later Versions
Cisco recommends that if you are using Cisco CME 3.0 or a later version, you should configure the transfer-system command using the full-consult or full-blind keyword, which allows IP phones to perform consultative or blind transfers to local phones and phones across a WAN. Prior to Cisco Unified CME 4.0, the default for the transfer-system command is the blind keyword, so the transfer-system command must be explicitly configured if you need the recommended full-consult or full-blind setting. In Cisco Unified CME 4.0 and later versions, the default for the transfer-system command is the full-consult keyword.

You can specify blind or consultative transfer on a systemwide basis using the transfer-system command. The systemwide setting can then be overridden for individual extensions using the transfer-mode command. For example, in a system that is set up for consultative transfer, a specific extension with an auto-attendant that automatically transfers incoming calls to specific extension numbers can be set to use blind transfer, because auto-attendants do not use consultative transfer.

Direct station select is a functionality that allows a multibutton phone user to transfer calls to an idle monitor line by pressing the Transfer key and the appropriate monitored line button. The dss keyword permits consultative call transfer to monitored lines.

Cisco ITS 2.1 and Earlier Versions
If you are using Cisco IOS Telephony Services (Cisco ITS) 2.1 or an earlier version, you should use the local-consult or blind keyword with the transfer-system command to enable the Cisco proprietary transfer method.

If you are using Cisco ITS 2.1, you can use the full-consult or full-blind keywords to enable H.450.2 call transfer by also configuring the router with a Tcl script that is contained in the file called app-h450-transfer.x.x.x.x.zip. This file is posted on the Cisco Unified CME software download website at http://www.cisco.com/cgi-bin/tablebuild.pl/ip-iostsp.

Consultative Transfer Support for Direct Station Select
For CME 3.2 and later versions, consultative transfers can take place during direct station select (transferring calls to idle monitor lines). The default behavior is a blind transfer. A monitored line is one that appears on two phones; one phone can use the line to make and receive calls and the other phone simply monitors whether the line is in use.

Consultative transfers to monitored lines are performed using the following steps:

Step 1 Answer the incoming call.
Step 2 Press the Transfer (transfer) soft key.
Step 3 If the monitor lamp is off, press the monitor-line button.
Step 4 Announce the call.
Step 5 Place the handset on hook or press the Transfer soft key a second time to transfer the call.
Call-Handling Features

Call Transfer

If the person sharing the monitor line does not want to accept the call, the person announcing the call can reconnect to the incoming call by pressing the EndCall soft key to terminate the announcement call and pressing the Resume soft key to reconnect to the original caller.

Direct station select consultative transfer is enabled with the addition of the dss keyword to the transfer-system full-consult command, which defines the call transfer method for all lines served by the router.

Note that the transfer-system full-consult dss command also supports the keep-conference command. See the “Conferencing” section on page 480.

Call Transfer Blocking

By default, transfers to all numbers except for those on local ephones are automatically blocked. During configuration, you can allow transfers to non-local numbers using the transfer-pattern (telephony-service) command. In Cisco Unified CME 4.0 and later versions, the transfer-pattern blocked command is provided to prevent individual phones from transferring calls to numbers that have been globally enabled for transfer using the transfer-pattern (telephony-service) command. By using the transfer-pattern blocked command, you can assure that individual ephones will not be able to incur toll charges by transferring calls outside the Cisco Unified CME system. The transfer-pattern blocked command can be used in ephone configuration mode for individual phones or in ephone-template configuration mode to become part of a template that is applied to a set of phones.

Another way to eliminate toll charges on call transfers is to limit the number of digits that phone users can dial when transferring calls. For example, if you use the transfer max-length command to specify a maximum of eight digits in the configuration, you are allowing users who are transferring calls to dial one digit for external access and seven digits more, which is generally enough for a local number but not a long-distance number. In most locations, this plan will limit transfers to non-toll destinations. Long-distance calls, which typically require ten digits or more, will not be allowed. This command is only necessary when global transfer to numbers outside the Cisco Unified CME system has been permitted using the transfer-pattern (telephony-service) command. Otherwise, transfers to numbers outside the Cisco Unified CME system are not permitted by default.

Note

Call transfers can also be made to speed-dial numbers by invoking the transfer function and then pressing a speed-dial number or code. Transfers that are made using speed-dial are not blocked when the transfer-pattern blocked command is used. Transfers that are made using speed-dial also are not blocked by the after-hours block pattern command.

Configuring Call Transfer

This procedure enables support for network calls that use the H.450.2 standard and allows you to optionally specify a range of allowable transfer destinations. It also allows you to override the global setting for blind or consultative transfer for individual ephone-dns and block transfers to external destinations by individual ephones. For a more complete discussion of call transfer configuration and network issues, see the “Call Transfer and Forwarding Across Networks” information module.

SUMMARY STEPS

1. enable
2. configure terminal
3. telephony-service
4. \texttt{transfer-system \{blind \| full-blind \| full-consult [dss] \| local-consult\}}
5. \texttt{transfer-pattern transfer-pattern [blind]}
6. \texttt{exit}
7. \texttt{ephone-dn dn-tag [dual-line]}
8. \texttt{transfer-mode \{blind \| consult\}}
9. \texttt{exit}
10. \texttt{ephone-template template-tag}
11. \texttt{transfer-pattern blocked}
12. \texttt{transfer max-length digit-length}
13. \texttt{exit}
14. \texttt{ephone phone-tag}
15. \texttt{ephone-template template-tag}
16. Repeat Step 14 through Step 16 for each phone on which you want transfer capability limited.

\textbf{DETAILED STEPS}

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Router&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> telephony-service</td>
<td>Enters telephony-service configuration mode.</td>
</tr>
<tr>
<td>Example: Router(config)#</td>
<td></td>
</tr>
</tbody>
</table>
Call Transfer Features

Step 4

transfer-system {blind | full-blind | full-consult [dss] | local-consult}

Example:
Router(config-telephony)# transfer-system
full-consult

Defines the call transfer method to allow call transfer with consultation for all lines served by the router. The default for Cisco Unified CME 4.0 and later versions is the full-consult keyword. The default for Cisco CME 3.4 and earlier versions is the blind keyword.

Cisco CME 3.0 and later versions should use the full-blind or full-consult keyword.

Cisco ITS 2.1 and earlier versions should use the local-consult or blind keyword. (Cisco ITS 2.1 can use the full-blind or full-consult keyword by also using the Tcl script in the file called app-h450-transfer.x.x.x.x.zip.)

Cisco Unified CME systems on SIP networks should use the full-blind or full-consult keyword. For more information about SIP, see the “Trunking Support” section on page 263 and the Cisco IOS SIP Configuration Guide.

- **blind**—Transfers calls without consultation with a single phone line using the Cisco-proprietary method. This is the default for all versions prior to Cisco Unified CME 4.0.

- **full-blind**—Transfers calls without consultation using H.450.2 standard methods.

- **full-consult**—Transfers calls with consultation using H.450.2 standard methods and a second phone line if available. The calls fall back to full-blind if a second line is unavailable. This is the default for Cisco Unified CME 4.0 and later versions.

- **dss**—Transfers calls with consultation to idle monitor lines. All other call-transfer behavior is identical to full-consult.

- **local-consult**—Transfers calls with local consultation using a second phone line if available. The calls fall back to blind for nonlocal consultation or nonlocal transfer target.

Note Systems using Cisco CME 3.0 or later versions must use this command with the full-consult or full-blind keyword to ensure compatibility with H.450 standards. Systems using Cisco Unified CME 4.0 or later versions do not have to explicitly configure this command because the full-consult keyword is the default.
### Command or Action

**Step 5**  
`transfer-pattern transfer-pattern [blind]`

**Example:**
```plaintext
Router(config-telephony)# transfer-pattern .T
```

<table>
<thead>
<tr>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allows transfer of telephone calls by Cisco Unified IP phones to specified phone number patterns. If no transfer pattern is set, the default is that transfers are permitted only to other local IP phones.</td>
</tr>
<tr>
<td>- <code>transfer-pattern</code>: String of digits for permitted call transfers. Wildcards are allowed. A pattern of .T transfers all calling parties using the H.450.2 standard.</td>
</tr>
<tr>
<td>- <code>blind</code>: (Optional) When H.450.2 consultative call transfer is configured, forces transfers that match the pattern specified in this command to be executed as blind transfers. Overrides settings made using the <code>transfer-system</code> and <code>transfer-mode</code> commands.</td>
</tr>
</tbody>
</table>

**Note:** When defining transfers to nonlocal numbers, it is important to note that transfer-pattern digit matching is performed before translation-rule operations. Therefore, you should specify in this command the digits actually entered by phone users before they are translated. For more information, see the “Translation Rules” section in the “SETTING UP PHONES” information module.

**Step 6**  
`exit`

**Example:**
```plaintext
Router(config-telephony)# exit
```

<table>
<thead>
<tr>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exits telephony-service configuration mode.</td>
</tr>
</tbody>
</table>

**Step 7**  
`ephone-dn dn-tag [dual-line]`

**Example:**
```plaintext
Router(config)# ephone-dn 20
```

<table>
<thead>
<tr>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enters ephone-dn configuration mode, creates an ephone-dn, and optionally assigns it dual-line status.</td>
</tr>
<tr>
<td>- <code>dn-tag</code>: Unique sequence number that identifies this ephone-dn during configuration tasks. The maximum number of ephone-dns for a particular Cisco Unified CME system is version- and platform-specific. Refer to CLI help for the range of values.</td>
</tr>
<tr>
<td>- <code>dual-line</code>: (Optional) Enables an ephone-dn with one voice port and two voice channels, which supports features such as call waiting, call transfer, and conferencing with a single ephone-dn.</td>
</tr>
</tbody>
</table>

**Step 8**  
`transfer-mode {blind | consult}`

**Example:**
```plaintext
Router(config-ephone-dn)# transfer-mode blind
```

<table>
<thead>
<tr>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Optional) Specifies the type of call transfer for an individual ephone-dn that uses the ITU-T H.450.2 standard, allowing you to override the global setting.</td>
</tr>
<tr>
<td>- <code>blind</code>: Transfers calls without consultation using a single phone line.</td>
</tr>
<tr>
<td>- <code>consult</code>: Transfers calls with consultation using a second phone line, if available.</td>
</tr>
</tbody>
</table>

**Step 9**  
`exit`

**Example:**
```plaintext
Router(config-ephone-dn)# exit
```

<table>
<thead>
<tr>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exits ephone-dn configuration mode.</td>
</tr>
<tr>
<td>Step</td>
</tr>
<tr>
<td>--------</td>
</tr>
<tr>
<td>10</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>11</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>12</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>13</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>14</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>15</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>16</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>17</td>
</tr>
</tbody>
</table>
Verifying Call Transfer

**Step 1** Use the `show running-config` command to verify your configuration. Transfer method and patterns are listed in the telephony-service portion of the output. You can also use the `show telephony-service` command to display this information.

```plaintext
Router# show running-config

! 
telephony-service
    fxo hook-flash
load 7910 P00403020214
load 7960-7940 P00305000600
load 7914 S00103020002
load 7905 CP7905040000SCCP040701A
max-ephones 100
max-dn 500
ip source-address 10.115.33.177 port 2000
max-redirect 20
no service directed-pickup
timeouts ringing 10
voicemail 7189
max-conferences 8 gain -6
moh music-on-hold.au
web admin system name cisco password cisco
dn-webedit
time-webedit
transfer-system full-consult
transfer-pattern 92.......
transfer-pattern 91.......... transfer-pattern 93.......
transfer-pattern 94......
transfer-pattern 95.......
transfer-pattern 96......
transfer-pattern 97.......
transfer-pattern 98......
transfer-pattern 99.......
transfer-pattern .T
secondary-dialtone 9
!
create cnf-files version-stamp 7960 Jul 13 2004 03:39:28
```

**Step 2** If you have used the `transfer-mode` command to override the global transfer mode for an individual ephone-dn, use the `show running-config` or `show telephony-service ephone-dn` command to verify that setting.

```plaintext
Router# show running-config

! 
ephone-dn 40 dual-line
number 451
description Main Number
huntstop channel
no huntstop
transfer-mode blind
```

**Step 3** To view ephone-template configurations, use the `show telephony-service ephone-template` command.
Examples

This section contains the following examples:

- **Basic Call Transfer: Example**, page 473
- **Call Transfer Blocking: Example**, page 473

**Basic Call Transfer: Example**

The following example sets all transfers that are initiated by a Cisco CME 3.1 or later system to use the H.450 standards.

```plaintext
telephony-service
    transfer-system full-consult
    transfer-pattern .T
```

**Call Transfer Blocking: Example**

The following example limits transfers from ephone 6, extension 2977, to numbers containing 8 digits or fewer.

```plaintext
telephony-service
    load 7910 P00403020214
    load 7960-7940 P00305000600
    load 7914 S00103020002
    load 7905 CP7905040000SCCP040701A
    load 7912 CP7912040000SCCP040701A
    max-ephones 100
    max-dn 500
    ip source-address 10.104.8.205 port 2000
    max-redirect 20
    system message XYZ Inc.
    create cnf-files version-stamp 7960 Jul 13 2004 03:39:28
    voicemail 7189
    max-conferences 8 gain -6
    moh music-on-hold.au
    web admin system name admin1 password admin1
    dn-webedit
    time-webedit
    transfer-system full-consult
    transfer-pattern 91...........
    transfer-pattern 92....... 
    transfer-pattern 93...... 
    transfer-pattern 94...... 
    transfer-pattern 95...... 
    transfer-pattern 96...... 
    transfer-pattern 97...... 
    transfer-pattern 98...... 
    transfer-pattern 99...... 
    secondary-dialtone 9
    fac standard
    ephone-template 2
    transfer max-length 8
    ephone-dn 4
    number 2977
    ephone 6
    button 1:4
    ephone-template 2
```
Troubleshooting Call Transfer

**Step 1** Use the `debug ephone` commands to observe messages and states associated with an ephone. For more information, see the *Cisco IOS Debug Command Reference*.

Feature History for Call Transfer

<table>
<thead>
<tr>
<th>Cisco Unified CME Version</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>Call transfer was introduced, using a Cisco-proprietary method.</td>
</tr>
<tr>
<td>2.1</td>
<td>Support was introduced for consultative transfer using the ITU-T H.450.2 standard.</td>
</tr>
<tr>
<td>3.0</td>
<td>Local hairpin call routing was supported as an option for networks that cannot support H.450 call transfer and forwarding. This feature requires installation of the Tcl script app_h450_transfer.2.0.0.8.tcl or a later version.</td>
</tr>
</tbody>
</table>
| 3.1                       | Support was introduced for the following:  
  - Enhancements for VoIP networks which contain a mix of platforms that support H.450.2 and H.450.3 standards, such as Cisco CME 3.1, Cisco CME 3.0, Cisco ITS V2.1, and platforms that do not support H.450.2 and H.450.3 standards, such as Cisco Unified CallManager, Cisco BTS Softswitch (BTS), and Cisco PSTN Gateway (PGW).  
  - H.450.12 standards.  
  - Automatic detection of Cisco Unified CallManager endpoints.  
  - Hairpin VoIP-to-VoIP call routing and routing to an H.450 tandem gateway. |
| 3.2                       | Consultative transfer to monitored lines using direct station select is introduced. |
| 4.0                       |  
  - Transfers to phones outside the Cisco Unified CME system can be blocked for individual ephones.  
  - The number of digits allowed for transfer destination numbers can be limited.  
  - The default for the `transfer-system` command was changed from the `blind` keyword to the `full-consult` keyword. |

Related Features

**Transfer Support**

More information about basic call transfer across the network can be found in the “Transfer and Forwarding Support” section on page 223.
Controlling Use of the Transfer Soft Key
To block the functioning of the call transfer (Transfer) soft key without removing the key display, create and apply an ephone template that contains the features blocked command. For more information, see the “Feature Control” section on page 329.

To remove the call transfer (Transfer) soft key from one or more phones, create and apply an ephone template that contains the appropriate softkeys command. For more information, see the “Soft-Key Display” section on page 551.

Caller ID Blocking

When Caller ID blocking is enabled, the display of caller information is prevented on outgoing calls. Caller ID blocking can be allowed on a per-call basis or can be enabled for individual ephone-dns under specific conditions. This section contains the following topics:

- Caller ID Blocking Overview, page 475
- Configuring Caller ID Blocking, page 476
- Verifying Caller ID Blocking, page 478
- Examples, page 479
- Feature History for Caller ID Blocking, page 480

Caller ID Blocking Overview

The following types of caller ID blocking are available for Cisco Unified CME systems:

- Caller ID Blocking per Call, page 475
- Caller ID Blocking on Outbound Calls, page 476

Caller ID Blocking per Call

The display of caller ID can be blocked for outgoing calls on a per-call basis, allowing users to maintain their privacy when necessary. The system administrator first defines a code for caller ID blocking in the system. Users can then dial the code prior to making any call on which they do not want their number displayed on the called-party phone. The caller ID is still sent, but its presentation parameter is set to “restricted” so that the caller ID is not displayed.

To enable caller ID blocking on a per-call basis, a system administrator defines a code using the caller-id block code command. Users then enter the code prior to making calls on which they do not want their number sent.
Caller ID Blocking on Outbound Calls

Using the commands in this section, you can block all caller-ID (CLID) displays on all calls from a particular ephone-dn, or you can selectively choose to block name, number, or both on outbound VoIP calls only.

To block all CLID displays for calls from a particular extension, use the **caller-id block** command in ephone-dn configuration mode. This command asks the far-end gateway device to block display of calling-party information for the calls received from this ephone-dn.

Alternatively, you can allow the local display of CLID information by not using the **caller-id block** command and independently block CLID name, CLID number, or both on outbound VoIP calls using the **clid strip** command in dial-peer configuration mode. This arrangement has the benefit of allowing caller-ID display for local calls while preventing caller-ID display for external calls going to VoIP.

This feature can also be used for public switched telephony network (PSTN) calls that go out over ISDN.

Restrictions

Caller ID blocking on outbound calls does not apply to PSTN calls that are made through foreign exchange office (FXO) ports. Caller ID features on FXO-connected subscriber lines are under the control of the PSTN service provider, who may require that you subscribe to their caller ID blocking service.

Configuring Caller ID Blocking

This procedure sets up a code that phone users can dial to block caller ID display per call and blocks caller ID displays from VoIP calls on a per-phone basis.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. telephony-service
4. caller-id block code *code-string*
5. exit
6. ephone-dn *dn-tag*
7. caller-id block
8. exit
9. dial-peer voice *tag* voip
   or
   dial-peer voice *tag* pots
10. clid strip
11. clid strip name
12. exit
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>enable</td>
</tr>
<tr>
<td>Example:</td>
<td>Router&gt; enable</td>
</tr>
<tr>
<td>Enables privileged EXEC mode.</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td>Example:</td>
<td>Router# configure terminal</td>
</tr>
<tr>
<td>Enters global configuration mode.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 1</strong></td>
<td>telephony-service</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config)# telephony-service</td>
</tr>
<tr>
<td>Enters telephony-service configuration mode.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>caller-id block code code-string</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-telephony)# caller-id block code *1234</td>
</tr>
<tr>
<td>(Optional) Defines a code that users can enter before making calls on which the caller ID should not be displayed.</td>
<td>• code-string—Digit string of up to 16 characters. The first character must be an asterisk (*).</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>exit</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-telephony)# exit</td>
</tr>
<tr>
<td>Exits telephony-service configuration mode.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 1</strong></td>
<td>ephone-dn dn-tag</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config)# ephone-dn 3</td>
</tr>
<tr>
<td>Enters ephone-dn configuration mode.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>caller-id block</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-ephone-dn)# caller-id block</td>
</tr>
<tr>
<td>(Optional) Blocks display of all caller-ID information for outbound calls that originate from this ephone-dn.</td>
<td>• By default, caller ID is not blocked on calls that originate from a Cisco Unified IP phone.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>exit</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-ephone-dn)# exit</td>
</tr>
<tr>
<td>Exits ephone-dn configuration mode.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>dial-peer voice tag voip</td>
</tr>
<tr>
<td>or</td>
<td>dial-peer voice tag pots</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config)# dial-peer voice 3 voip</td>
</tr>
<tr>
<td>or</td>
<td>Router(config)# dial-peer voice 5 pots</td>
</tr>
<tr>
<td>Enters dial-peer configuration mode.</td>
<td><strong>Note</strong> You can configure caller-ID blocking on POTS dial peers if the POTS interface is ISDN. This feature is not available on FXO/CAS lines.</td>
</tr>
</tbody>
</table>
Verifying Caller ID Blocking

Step 1  Use the show running-config command to display caller ID blocking parameters, which may appear in the telephony-service, ephone-dn, or dial-peer portions of the output.

Router# show running-config

dial-peer voice 450002 voip
  translation-profile outgoing 457-456
  destination-pattern 457
  session target ipv4:10.43.31.81
  dtmf-relay h245-alphanumeric
  codec g711ulaw
  no vad
  clid strip

!  telephony-service
  fxo hook-flash
  load 7960-7940 P00305000600
  load 7914 S00103020002
  max-ephones 100
  max-dn 500
  ip source-address 10.115.34.131 port 2000
  max-redirect 20
  no service directed-pickup
  timeouts ringing 10
  system message XYZ Company
  voicemail 7189
  max-conferences 8 gain -6
  moh music-on-hold.au
  caller-id block code *1234
  web admin system name cisco password cisco
dn-webedit
  time-webedit
  transfer-system full-consult
  transfer-pattern 92......
  transfer-pattern 91...........
  transfer-pattern 93......
  transfer-pattern 94......
  transfer-pattern 95......
  transfer-pattern 96......
Caller ID Blocking

Examples

This section contains the following examples:

- Caller ID Blocking Code: Example, page 479
- Caller ID Blocking for Outgoing Calls: Example, page 479

**Caller ID Blocking Code: Example**

The following example defines a code of *1234 for users to enter to block caller ID on their outgoing calls:

```
telephony-service
caller-id block code *1234
```

**Caller ID Blocking for Outgoing Calls: Example**

The following example sets CLID blocking for the ephone-dn with tag 3.

```
ephone-dn 3
  number 2345
  caller-id block
```

The following example blocks the display of CLID name and number on VoIP calls but allows CLID display for local calls:

```
ephone-dn 3
  number 2345
dial-peer voice 2 voip
clid strip
clid strip name
```
Feature History for Caller ID Blocking

<table>
<thead>
<tr>
<th>Cisco Unified CME Version</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>Caller ID blocking was introduced.</td>
</tr>
<tr>
<td>3.0</td>
<td>Caller ID blocking per call was introduced.</td>
</tr>
</tbody>
</table>

Conferencing

Conferencing allows you to join three parties in a telephone conversation. This section describes the following topics:

- Conferencing Overview, page 480
- Configuring Conferencing, page 482
- Verifying Conferencing, page 485
- Examples, page 485
- Troubleshooting Conferencing, page 486
- Feature History for Conferencing, page 487
- Related Features, page 487

Conferencing Overview

Note

For a summary of the functionality introduced in different releases, see the “Feature History for Conferencing” section on page 487.

Cisco Unified CME supports three-party conferences for local and on-net calls using a G.711 codec. This service supports conversion between G.711 mu-law and A-law and between G.711 and G.729. To allow callers who use a G.729 codec to join a conference, you need to specify the transcoding of G.729 to G.711 by using the `dspfarm-assist` keyword with the `codec` command, which allows the use of DSP resources on the router. DSP resources are limited, however, and there are disadvantages to using them for conferencing. For more information, see the “Codec (G.711 or G.729r8)” section on page 144 and the “Transcoding Support” section on page 199.

The maximum number of simultaneous conferences is platform-specific to the type of Cisco Unified CME router, and each individual Cisco Unified IP phone can host a maximum of one conference at a time. You cannot create a second conference on a phone if you already have an existing conference on hold.

This overview discusses the following topics:

- Conference Gain Levels, page 481
- End-of-Conference Options, page 481
Conference Gain Levels

In Cisco 3.3 and later releases, you can adjust the gain level of an external call to provide more adequate volume. This functionality is applied to inbound audio packets so that conference participants can more clearly hear a remote PSTN or VoIP caller joining their call. Note that this functionality cannot discriminate between a remote VoIP/foreign exchange office (FXO) source, which requires a volume gain, and a remote VoIP/IP phone, which does not require a volume gain and may therefore incur some sound distortions.

End-of-Conference Options

For Cisco CME 3.2 and later versions, a person who initiates a conference call and hangs up can either keep the remaining parties connected or disconnect them.

The `keep-conference` and `keep-conference endcall` commands configure IP phones to keep the remaining conference parties connected when the conference initiator hangs up (places the handset back in the on-hook position). Conference originators can disconnect from their conference calls by pressing the Confrn (conference) soft key. When an initiator uses the Confrn key to disconnect from the conference call, the oldest call leg will be put on hold, leaving the initiator connected to the most recent call leg. The conference initiator can then navigate between the two parties by pressing either the Hold soft key or the line buttons to select the desired call.

The `keep-conference` command causes the remote conference parties to remain connected when the conference initiator hangs up the phone and to disconnect the conference parties if the initiator presses the EndCall soft key. The `keep-conference endcall` command causes the remote conference parties to remain connected when the conference initiator hangs up or presses the EndCall soft key.

Conference initiator dropoff can be configured per ephone.

In Cisco Unified CME 4.0 and later versions, behavior for the end of three-way conferences can be specified using new options for the `keep-conference` command that can be configured per ephone. The options specify whether the last party that joined a conference can be dropped from the conference and whether the remaining two parties should be allowed to continue their connection after the conference initiator has left the conference. All options except the `no keep-conference` command can be combined to specify different behavior patterns. See the “Examples” section on page 485 for examples of combined options.

Note

This feature uses call transfer to connect the two remaining parties of a conference when a conference initiator leaves the conference. To use this feature, you must the `transfer-system` command must be configured with the `full-blind`, `full-consult`, or `full-consult dss` keywords. For Cisco Unified CME 4.0 and later versions, the `full-consult` keyword is the default. Users of other versions must explicitly configure an appropriate keyword.

Restrictions

Once a three-way conference has been established, a participant cannot use call transfer to join the remaining conference participants to a different number.
Configuring Conferencing

This procedure sets the maximum number of conferences and the conference gain, as well as any optional end-of-conference options.

SUMMARY STEPS

1. enable
2. configure terminal
3. telephony-service
4. max-conferences max-conference-number [gain -6 | 0 | 3 | 6]
5. exit
6. ephone phone-tag
7. keep-conference [drop-last] [endcall] [local-only]
8. exit
9. Repeat Step 6 through Step 8 for each ephone to receive end-of-conference options.

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
• Enter your password if prompted. |
| **Example:** | Router> enable |
| **Step 2** configure terminal | Enters global configuration mode. |
| **Example:** | Router# configure terminal |
| **Step 3** telephony-service | Enters telephony-service configuration mode. |
| **Example:** | Router(config)# |
### Call-Handling Features

#### Conferencing

**Step 4**

```
max-conferences max-conference-number
[gain -6 | 0 | 3 | 6]
```

Example:

```
Router(config-telephony)# max-conferences 6
```

Sets the maximum number of simultaneous three-party conferences supported by the router.

- **max-conference-number**—Maximum number of simultaneous three-party conferences supported by a router, which is platform-dependent. The default is half of the maximum number. The maximum number of conferences per platform is as follows:
  - Cisco 2600 series, Cisco 2801—8
  - Cisco 2811, Cisco 2821, Cisco 2851, Cisco 3600 series, Cisco 3700 series—16
  - Cisco 3800 series—24 (requires Cisco IOS Release 12.3(11)XL or higher)

- **gain**—(Optional) Amount to increase the sound volume of VoIP and PSTN calls joining a conference call, in decibels. Valid values are -6, 0, 3, and 6. The default is -6.

**Step 5**

```
exit
```

Example:

```
Router(config-telephony)# exit
```

Exits telephony-service configuration mode.

**Step 6**

```
ephone phone-tag
```

Example:

```
Router(config)# ephone 1
```

Enters ephone configuration mode.

- **phone-tag**—Unique sequence number that identifies this ephone during configuration tasks.
### Step 7

**Command or Action**

```
keep-conference [drop-last] [endcall] [local-only]
```

**Example:**

```
Router(config-ephone)# keep-conference endcall
```

**Purpose**

(Optional) Allows conference initiators to exit from conference calls and to either end or maintain the conference for the remaining parties.

- **no keep-conference**—(Default; the *no* form of the command) The conference initiator can hang up or press the EndCall soft key to end the conference and disconnect all parties or press the Confrn soft key to drop only the last party that was connected to the conference.

- **keep-conference**—(No keywords used) The conference initiator can press the EndCall soft key to end the conference and disconnect all parties or hang up to leave the conference and keep the other two parties connected. The conference initiator can also use the Confrn soft key (IP phone) or hookflash (analog phone) to break up the conference but stay connected to both parties.

- **drop-last**—The action of the Confrn soft key is changed; the conference initiator can press the Confrn soft key (IP phone) or hookflash (analog phone) to drop the last party.

**Note**

Analog phones connected to the Cisco Unified CME system through a Cisco VG 224 require Cisco IOS Release 12.3(11)YL1 or a later release to use this feature.

- **endcall**—The action of the EndCall soft key is changed; the conference initiator can hang up or press the EndCall soft key to leave the conference and keep the other two parties connected.

- **local-only**—The conference initiator can hang up to end the conference and leave the other two parties connected only if one of the remaining parties is local to the Cisco Unified CME system (an internal extension).

### Step 8

**exit**

**Example:**

```
Router(config-ephone)# exit
```

**Purpose**

Exits ephone configuration mode.

### Step 9

**Repeat** Step 6 through Step 8 for each ephone to receive end-of-conference options.
Verifying Conferencing

**Step 1** Use the `show running-config` command to verify your configuration. Any non-default conferencing parameters are listed in the telephony-service portion of the output, and end-of-conference options are listed in the ephone portion.

```
Router# show running-config

!  
ephone-dn 1 dual-line
ring feature secondary
number 126 secondary 1261
description Sales
name Smith
call-forward busy 500 secondary
call-forward noan 500 timeout 10
huntstop channel
no huntstop
no forward local-calls
!
ephone 1
mac-address 011F.92A0.C10B
type 7960 addon 1 7914
no dnd feature-ring
keep-conference
```

Examples

This section contains the following examples:

- Basic Conferencing: Example, page 485
- End of Conference Options: Example, page 485

**Basic Conferencing: Example**

The following example sets the maximum number of conferences for a Cisco Unified IP phone to 4 and configures a gain of 6 db for inbound audio packets from remote PSTN or VoIP calls joining a conference:

```
telephony-service
 max-conferences 4 gain 6
```

**End of Conference Options: Example**

In the following example, extension 3555 initiates a three-way conference. After the conference is established, extension 3555 can press the Confrn soft key to disconnect the last party that was connected and remain connected to the first party that was connected. If extension 3555 hangs up from the conference, the other two parties remain connected if one of them is local to the Cisco Unified CME system.

```
ephone-dn 35
 number 3555

ephone 24
 button 1:35
 keep-conference drop-last local-only
```
In the following example, extension 3666 initiates a three-way conference. After the conference is established, extension 3666 can press the Confrn soft key to disconnect the last party that was connected and remain connected to the first party that was connected. Also, extension 3666 can hang up or press the EndCall soft key to leave the conference and keep the other two parties connected.

```
ephone-dn 36
   number 3666

ephone 25
   button 1:36
   keep-conference drop-last endcall
```

In the following example, extension 3777 initiates a three-way conference. After the conference is established, extension 3777 can press the Confrn soft key to disconnect the last party that was connected and remain connected to the first party that was connected. Also, extension 3777 can hang up or press the EndCall soft key to leave the conference and keep the other two parties connected only if one of the two parties is local to the Cisco Unified CME system.

```
ephone-dn 38
   number 3777

ephone 27
   button 1:38
   keep-conference drop-last endcall local-only
```

In the following example, extension 3999 initiates a three-way conference. After the conference is established, extension 3999 can hang up or press the EndCall soft key to leave the conference and keep the other two parties connected only if one of the two parties is local to the Cisco Unified CME system. Extension 3999 can also use the Confrn soft key to break up the conference but stay connected to both parties.

```
ephone-dn 39
   number 3999

ephone 29
   button 1:39
   keep-conference endcall local-only
```

**Troubleshooting Conferencing**

**Step 1** Use the `debug ephone` commands to observe messages and states associated with an ephone. For more information, see the *Cisco IOS Debug Command Reference*. 
Feature History for Conferencing

<table>
<thead>
<tr>
<th>Cisco Unified CME Version</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.0</td>
<td>Support for conferencing was introduced.</td>
</tr>
<tr>
<td>3.2</td>
<td>Conference initiator drop-off control was introduced.</td>
</tr>
<tr>
<td>3.2.2</td>
<td>Conference gain control for external calls was introduced.</td>
</tr>
</tbody>
</table>
| 4.0                      | • End-of-conference options were introduced.  
|                           | • Phones connected in a three-way conference display “Conference.” |

Related Features

Controlling Use of the Conference Soft Key

To block the functioning of the conference (Confrrn) soft key without removing the key display, create and apply an ephone template that contains the features blocked command. For more information, see the “Feature Control” section on page 329.

To remove the conference (Confrrn) soft key from one or more phones, create and apply an ephone template that contains the appropriate softkeys command. For more information, see the “Soft-Key Display” section on page 551.
Phone Features

This chapter describes the following features that affect the appearance or operation of IP phones:

Phone Answering and Dialing Features
- Account Code Entry, page 492
- Automatic Line Selection, page 493
- Callback Busy Subscriber, page 496
- Class of Restriction, page 497
- Distinctive Ringing, page 502
- Do Not Disturb, page 504
- Headset Auto-Answer, page 508
- Intercom, page 513
- MWI Line Selection, page 519
- On-Hook Dialing, page 522
- Speed Dial, page 523

Phone Display Features
- Called-Name Display, page 537
- Ephone-dn Labels, page 545
- Phone Header Bar Display, page 547
- Soft-Key Display, page 551
- System Message Display, page 557

Phone Functions Features
- Flash Soft Key, page 561
- PC Port Disable, page 564
- URL Provisioning for Customized Function Buttons, page 569
Phone Features Overview

The features in this information module allow you to modify the displays and functionality of IP phones at your site. Table 31 summarizes these features.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Benefit</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Account Code Entry</strong></td>
<td>When an account code is entered for a call, the system inserts the account code into call-detail records and management reports.</td>
<td>Administrators can associate calls with accounts.</td>
<td>A lawyer calls a client and enters the account code for that client. Later, the call charges can be billed to the client.</td>
</tr>
<tr>
<td><strong>Automatic Line Selection</strong></td>
<td>System chooses a line based on the configuration for the ephone.</td>
<td>System administrators can define individual phone answering and line selection behaviors as appropriate.</td>
<td>A phone user has a line for outgoing calls on the third button and has set automatic line selection to this button, so whenever the handset is picked up, the line on the third button is automatically used.</td>
</tr>
<tr>
<td><strong>Callback Busy Subscriber</strong></td>
<td>System sets an notification alert when a user attempts to call a line that is busy. When the line is free, the system notifies the user who tried to call.</td>
<td>Phone users are notified when busy extensions are free and do not have to continually retry them.</td>
<td>Mary in Sales attempts to call Rita in Scheduling to arrange a delivery but Rita’s line is busy. Mary presses the CallBack soft key, and when Rita hangs up, Mary is notified.</td>
</tr>
<tr>
<td><strong>Class of Restriction</strong></td>
<td>System restricts certain dial peers access to other dial peers based on the configuration.</td>
<td>System administrators can block certain types of calls from specified extensions.</td>
<td>Phone users at lobby phones are unable to make long-distance calls.</td>
</tr>
<tr>
<td><strong>Distinctive Ringing</strong></td>
<td>System uses different ring patterns for internal calls, external calls, and feature notifications.</td>
<td>Phone users can identify the type of call before they look at their phone displays.</td>
<td>John is working on a report and only wants to take calls from external customers. He recognizes the internal ring and allows those calls to be forwarded to voice mail.</td>
</tr>
</tbody>
</table>

Note: For more information about Cisco IOS voice features, see the entire Cisco IOS Voice Configuration Library—including library preface and glossary, feature documents, and troubleshooting information—at http://www.cisco.com/en/US/products/ps6441/prod_configuration_guide09186a0080565f8a.html.
**Table 31  Phone Features Summary (Continued)**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Benefit</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do Not Disturb</td>
<td>System doesn’t ring a phone for incoming calls when DND is active.</td>
<td>Phone users can press a DND soft key or use a DND feature access code to keep calls from ringing at the phone. DND can be bypassed for lines designated for feature ring. Calls are forwarded if no-answer call forwarding is configured.</td>
<td>John is working on a report and only wants to take calls from his family on his private line, which has been designated for feature ringing. He presses DND and all his other calls are forwarded to voice mail.</td>
</tr>
<tr>
<td>Headset Auto-Answer</td>
<td>System connects calls automatically to lines that are specified for headset auto-answer.</td>
<td>Phone users do not need to press phone buttons to answer incoming calls when they have their headsets engaged.</td>
<td>A phone agent answers incoming calls for a charity organization. The calls are automatically connected whenever the agent activates the headset key.</td>
</tr>
<tr>
<td>Intercom</td>
<td>System sets up a dedicated two-way audio path between two phones.</td>
<td>Phone users who frequently need to speak to each other always have a path available, even if one of them is using the phone.</td>
<td>A cashier needs to authorize all purchases over $100 with the manager, and uses the intercom to get approvals without having to wait until the manager’s phone is free.</td>
</tr>
<tr>
<td>MWI Line Selection</td>
<td>System monitors a phone line other than the primary line for messages waiting in a voice-mail system.</td>
<td>Phone users can see and respond to waiting messages on a line other than their primary line.</td>
<td>A phone user wants to know when messages are waiting for the second line on a phone rather than the first line.</td>
</tr>
<tr>
<td>On-Hook Dialing</td>
<td>System recognizes digits dialed prior to the handset being taken off hook.</td>
<td>Phone users can begin dialing without removing the handset.</td>
<td>A phone user dials four digits, lifts the handset, and hears the called extension ringing.</td>
</tr>
<tr>
<td>Speed Dial</td>
<td>System dials complete telephone numbers that have been associated with buttons or abbreviated numbers.</td>
<td>Phone users can dial faster and often without looking up the number of a frequently called phone.</td>
<td>A phone user presses a phone button that has been programmed for speed dial and a ten-digit number is dialed.</td>
</tr>
</tbody>
</table>

**Display Features**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Benefit</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Called-Name Display</td>
<td>System displays directory name or ephone name instead of called number.</td>
<td>Phone agents who answer calls for multiple parties are presented with the name of the party for whom the call is intended.</td>
<td>An answering service answers calls for three doctors using one line. For each incoming call, the phone displays the name of the doctor who was called.</td>
</tr>
<tr>
<td>Ephone-dn Labels</td>
<td>System displays the specified text string instead of the extension number next to an ephone-dn line button.</td>
<td>Phone users with multiple line buttons can have names next to their line buttons rather than extension numbers.</td>
<td>A receptionist’s phone with ten line buttons has names next to each button rather than numbers.</td>
</tr>
</tbody>
</table>
Table 31  Phone Features Summary (Continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Benefit</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phone Header Bar Display</td>
<td>System displays text associated with the first ephone-dn in the top line of the phone display.</td>
<td>Phone users can see alternative information that is specific to their first phone line, such as the complete phone number for that line.</td>
<td>A phone displays extension number 122 next to the first line button and displays (408) 555-0122 in the phone header bar.</td>
</tr>
<tr>
<td>Soft-Key Display</td>
<td>System displays soft keys as configured by the user.</td>
<td>System administrators can limit or rearrange soft keys based on their needs or policies.</td>
<td>Phones in the public lobbies have had many of their soft keys, such as Transfer and PickUp, removed to prevent misuse of the phone system by unauthorized people.</td>
</tr>
<tr>
<td>System Message Display</td>
<td>System displays custom text or HTML file in phone displays when phones are idle.</td>
<td>Systemwide or corporate messages can be transmitted to all phone users.</td>
<td>A text message reminding employees of an end-of-the-quarter deadline for timesheets is sent to all phones.</td>
</tr>
</tbody>
</table>

Phone Functions Features

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Benefit</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flash Soft Key</td>
<td>System sends hookflash signal when Flash soft key is pressed.</td>
<td>Phone user can use PSTN features that require hookflash.</td>
<td>A phone user presses Flash to send a hookflash signal to add a party to a conference with a PSTN host.</td>
</tr>
<tr>
<td>PC Port Disable</td>
<td>System deactivates the PC port on individual IP phones.</td>
<td>System administrators can prevent PCs from being connected to certain phones.</td>
<td>A phone in a corporate lobby has had its PC port disabled to prevent unauthorized people from using the port to access the data network.</td>
</tr>
<tr>
<td>URL Provisioning for Customized Function Buttons</td>
<td>System uses configured URLs to find XML files that provision phone function buttons instead of the default.</td>
<td>System administrators can provide custom directory or other services as needed.</td>
<td>A site-specific help file is provided from the Information function button.</td>
</tr>
</tbody>
</table>

Account Code Entry

Account Code Entry allows phone users to enter an account code from the phone keypad which will be associated with the current call in call-detail records and management reports. This section describes the following topics:

- Account Code Entry Overview, page 493
- Feature History for Account Code Entry, page 493
Account Code Entry Overview

The Cisco Unified IP Phones 7940 and 7940G and the Cisco Unified IP Phones 7960 and 7960G allow users to enter account codes during call setup or while connected to an active call using the Acct soft key. Account codes are inserted into call detail records (CDRs) on the Cisco Unified CME router for later interpretation by billing software.

An account code is visible in the output of the show call active command and the show call history command for telephony call legs and is supported by the CISCO-VOICE-DIAL-CONTROL-MIB. The account code also appears as a named string of “account-code” in RADIUS vendor-specific attribute (VSA) Vendor Type field 1 for voice authentication, authorization, and accounting (AAA) accounting.

No configuration is required for this feature. To enter an account code during call setup or while in a connected state, press the Acct soft key and enter the account code from the phone keypad.

Feature History for Account Code Entry

<table>
<thead>
<tr>
<th>Cisco Unified CME Version</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.0</td>
<td>Account code entry was introduced.</td>
</tr>
</tbody>
</table>

Automatic Line Selection

Automatic Line Selection allows you to specify, on a per-phone basis, the line that is selected when you pick up a phone handset. This section describes the following topics:

- Automatic Line Selection Overview, page 493
- Configuring Automatic Line Selection, page 494
- Verifying Automatic Line Selection, page 495
- Examples, page 496
- Feature History for Automatic Line Selection, page 496

Automatic Line Selection Overview

Note

For a summary of the functionality introduced in different releases, see the “Feature History for Automatic Line Selection” section on page 496.

For a multiline phone, it is often useful to set up the phone so that lifting the handset automatically selects the first ringing line on the phone or, if no line is ringing, selects the first available idle line on the phone. This is the behavior of all multiline IP phones before Cisco Unified CME 3.0.

Under some circumstances, however, you might want to specify that a line button must be explicitly pressed to select an outgoing line or to answer an incoming call. Starting in Cisco CME 3.0, you have the flexibility to assign the type of line selection that each IP phone employs.
Any of the following behaviors can be assigned on a per-phone basis:

- **Automatic line selection**—Picking up the handset answers the first ringing line or, if no line is ringing, selects the first idle line. Use the `auto-line` command with no keyword or argument.
- **Manual line selection (no automatic line selection)**—Pressing the Answer soft key answers the first ringing line, and pressing a line button selects a line for an outgoing call. Picking up the handset does not answer calls or provide dial tone. Use the `no auto-line` command.
- **Automatic line selection for incoming calls only**—Picking up the handset answers the first ringing line, but if no line is ringing, it cannot select an idle line for an outgoing call. Pressing a line button selects a line for an outgoing call. Use the `auto-line incoming` command.
- **Automatic line selection for outgoing calls only**—Picking up the handset selects the line that has been configured for this purpose with the `auto-line` command and the `button-number` argument in Cisco CME 3.1 and later versions. If a button number has been specified and the line associated with that button is unavailable (because it is a shared line in use on another phone), no dial tone is heard when the handset is lifted and you must press an available line button to make an outgoing call. This feature does not apply to incoming calls, which must be answered by pressing the Answer soft key or a ringing line button.

## Configuring Automatic Line Selection

This procedure allows you to specify, for individual phones, the line that will be used when a handset is picked up.

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
   1. `ephone phone-tag`
   2. `[no] auto-line [incoming] [button-number]`
3. `exit`

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 1</strong> ephone phone-tag</td>
<td>Enters ephone configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# ephone 24</td>
<td>• <code>phone-tag</code>—Unique sequence number for the phone on which you want to configure automatic line selection.</td>
</tr>
</tbody>
</table>
Step 2

**Example:**

Router(config-ephone)# no auto-line

**Purpose**

Assigns a type of line selection behavior to this phone.

- **auto-line**—Picking up a handset answers the first ringing line or, if no line is ringing, selects the first idle line. This is also the default if this command is not used.
- **no auto-line**—Pressing the Answer soft key answers the first ringing line, and pressing a line button selects a line for an outgoing call. Picking up the handset does not answer calls or provide dial tone.
- **auto-line incoming**—Picking up the handset answers the first ringing line but, if no line is ringing, does not select an idle line for an outgoing call. Pressing a line button selects a line for an outgoing call.
- **auto-line button-number**—For Cisco CME 3.1 and later versions, picking up the handset selects the line associated with the that has been specified with this command during configuration. The default if this argument is not used is the topmost available line.

Step 3

**Example:**

Router(config-ephone)# exit

**Purpose**

Exits ephone configuration mode.

### Verifying Automatic Line Selection

**Step 1**

Use the `show running-config` command to verify your configuration. Automatic line selection is listed in the ephone portion of the output.

```
Router# show running-config

ephone 2
  headset auto-answer line 1
  headset auto-answer line 4
  ephone-template 1
  mac-address 011F.9010.1790
  paging-dn 48
  type 7960
  no dnd feature-ring
  no auto-line!
```

**Step 2**

Use the `show telephony-service ephone` command to display only ephone configuration information.

```
Router# show telephony-service ephone-dn

ephone 4
  device-security-mode none
  username "Accounting"
  mac-address FF0E.4857.5E91
  button 1c34,35
  no auto-line
```
Examples

The following example assigns no automatic line selection to phones 1 and 2 and assigns automatic line selection for incoming calls only to phone 3:

```
ephone 1
  mac-address 00e0.8646.9242
  button 1:1 2:4 3:16
  no auto-line

ephone 2
  mac-address 01c0.4612.7142
  button 1:5 2:4 3:16
  no auto-line

ephone 3
  mac-address 10b8.8945.3251
  button 1:6 2:4 3:16
  auto-line incoming
```

Feature History for Automatic Line Selection

<table>
<thead>
<tr>
<th>Cisco Unified CME Version</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.0</td>
<td>Automatic line selection was introduced.</td>
</tr>
<tr>
<td>3.1</td>
<td>The ability to select a button other than the topmost button was introduced.</td>
</tr>
</tbody>
</table>

Callback Busy Subscriber

This feature allows you to place a notification request on a busy extension to let you know when the extension becomes free. This section describes the following topics:

- Callback Busy Subscriber Overview, page 496
- Troubleshooting Callback Busy Subscriber, page 497
- Feature History for Callback Busy Subscriber, page 497

Callback Busy Subscriber Overview

This feature allows callers who dial a busy extension number to request a callback from the system when a called number that was busy is free. Callers can also request callbacks for extensions that do not answer, and the system will notify them after the called phone is next used.

This feature is available only on the Cisco Unified Wireless IP Phone 7920, Cisco Unified IP Phones 7940 and 7940G, and Cisco Unified IP Phones 7960 and 7960G.

To activate the callback feature after dialing an extension number and hearing a busy or no-answer tone, press the CallBack soft key. When the system calls back to notify you that the called line is free, the phone rings once, briefly, and displays “CallBack Redial” and the extension number. To call the number, press the Redial soft key.
There can be only one callback request pending against a particular extension number, although one caller may initiate a number of callbacks to different numbers. If a caller attempts to place a callback request on a number that already has a pending callback request, the caller hears a fast-busy tone.

If the called number has call forwarding enabled, the callback request is placed against the final destination number.

No configuration is required for this feature.

Troubleshooting Callback Busy Subscriber

**Step 1** Use the `show ephone-dn callback` command to list the phones that have pending callback requests against them.

```
Router# show ephone-dn callback
DN 3 (95021) CallBack pending to DN 1 (95021) for ephone-1 age 7 seconds
State for DN 3 is CH1 HOLD CH2 SIEZE
```

Feature History for Callback Busy Subscriber

<table>
<thead>
<tr>
<th>Cisco Unified CME Version</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.0</td>
<td>Callback busy subscriber was introduced.</td>
</tr>
</tbody>
</table>

Class of Restriction

Class of Restriction (COR) provides system administrators with a way to restrict certain types of calls from specific extensions. This section describes the following topics:

- Class of Restriction Overview, page 498
- Configuring Class of Restriction, page 498
- Verifying Class of Restriction, page 499
- Examples, page 499
- Troubleshooting Class of Restriction, page 500
- Feature History for Class of Restriction, page 501
- Related Features, page 501
Class of Restriction Overview

Note
For a summary of the functionality introduced in different releases, see the “Feature History for Class of Restriction” section on page 501.

Class of restriction (COR) is used to specify which incoming dial peer can use which outgoing dial peer to make a call. Each dial peer can be provisioned with an incoming and an outgoing COR list. The `corlist` command sets the dial-peer COR parameter for dial peers and the directory numbers that are created for Cisco Unified IP phones associated with the Cisco Unified CME router. COR functionality provides the ability to deny certain call attempts on the basis of the incoming and outgoing class of restrictions that are provisioned on the dial peers. This functionality provides flexibility in network design, allows users to block calls (for example, calls to 900 numbers), and applies different restrictions to call attempts from different originators.

For more information on setting COR, refer to the “Class of Restrictions” section in the “Dial Peer Configuration on Voice Gateway Routers” chapter in the Cisco IOS Voice Configuration Library.

Configuring Class of Restriction

This procedure applies a class of restriction to the dial peers associated with a Cisco Unified CME ephone-dn.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. ephone-dn *dn-tag*
4. corlist `{incoming | outgoing}` *cor-list-name*
5. exit

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
  - Enter your password if prompted. |
| **Example:** Router> enable | |
| **Step 2** configure terminal | Enters global configuration mode. |
| **Example:** Router# configure terminal | |
| **Step 3** ephone-dn *dn-tag* | Enters ephone-dn configuration mode.  
  - *dn-tag*—The unique sequence number for the ephone-dn to which you want to apply a COR. |
| **Example:** Router(config)# ephone-dn 12 | |
Verifying Class of Restriction

Step 1
Use the `show running-config` command or the `show telephony-service ephone-dn` command to verify whether the COR lists have been applied to the appropriate ephone-dns.

Router# show running-config

ephone-dn 23
  number 2835
  corlist outgoing 5x

Examples

The following example shows three dial peers for dialing local destinations, long distance, and 911. COR list user1 can access the dial peers used to call 911 and local destinations. COR list user2 can access all three dial peers. Ephone-dn 1 is assigned COR list user1 to call local destinations and 911, and ephone-dn 2 is assigned COR list user2 to call 911, local destinations, and long distance.

dial-peer cor custom
  name local
  name longdistance
  name 911

dial-peer cor list call-local
  member local

dial-peer cor list call-longdistance
  member longdistance

dial-peer cor list call-911
  member 911

dial-peer cor list user1
  member 911
  member local

dial-peer cor list user2
  member 911
  member local
  member longdistance
dial-peer voice 1 pots
corlist outgoing call-longdistance
destination-pattern 91...........
port 2/0/0

dial-peer voice 2 pots
corlist outgoing call-local
destination-pattern 9[2-9]......
port 2/0/0

dial-peer voice 3 pots
corlist outgoing call-911
destination-pattern 9911
port 2/0/0

ephone-dn 1
corlist incoming user1
corlist outgoing user1

ephone-dn 2
corlist incoming user2
corlist outgoing user2

## Troubleshooting Class of Restriction

### Step 1

Use the `show dialplan dialpeer` command to determine which outbound dial peer is matched for an incoming call, based on the COR criteria and dialed number specified in the command line. Use the `timeout` keyword to enable matching variable-length destination patterns associated with dial peers. This can increase your chances of finding a match for the dial peer number you specify.

Router# `show dialplan dialpeer 300 number 1900111`

VoiceOverIpPeer900

```
information type = voice,
description = '',
tag = 900, destination-pattern = '1900',
answer-address = '', preference=0,
numbering Type = 'unknown'
group = 900, Admin state is up, Operation state is up,
ing incoming called-number = '', connections/maximum = 0/unlimited,
DTMF Relay = disabled,
modem passthrough = system,
huntstop = disabled,
in bound application associated: 'DEFAULT'
out bound application associated: ''
dnis-map =
permission :both
incoming COR list:maximum capability
outgoing COR list:to900
type = voip, session-target = 'ipv4:1.8.50.7',
technology prefix:
settle-call = disabled
...
Time elapsed since last clearing of voice call statistics never
Connect Time = 0, Charged Units = 0,
Successful Calls = 0, Failed Calls = 0, Incomplete Calls = 0
Accepted Calls = 0, Refused Calls = 0,
Last Disconnect Cause is '',
```
Step 2  Use the display dial-peer voice command to display the attributes associated with a particular dial peer.

Router# show dial-peer voice 100

VoiceEncapPeer100
  information type = voice,
  description = '',
  tag = 100, destination-pattern = '',
  answer-address = '', preference=0,
  numbering Type = 'unknown'
  group = 100, Admin state is up, Operation state is up,
  Outbound state is up,
  incoming called-number = '555....', connections/maximum = 0/unlimited,
  DTMF Relay = disabled,
  huntstop = disabled,
  in bound application associated: 'vxml_inb_app'
  out bound application associated: ''
  dnis-map =
  permission :both
  incoming COR list:maximum capability
  outgoing COR list:minimum requirement
  type = pots, prefix = '',
  forward-digits default
  session-target = '', voice-port = '',
  direct-inward-dial = disabled,
  digit_strip = enabled,
  register E.164 number with GK = TRUE

  Connect Time = 0, Charged Units = 0,
  Successful Calls = 0, Failed Calls = 0, Incomplete Calls = 0
  Accepted Calls = 0, Refused Calls = 0,
  Last Disconnect Cause is '',
  Last Disconnect Text is '',
  Last Setup Time = 0.

---

Feature History for Class of Restriction

<table>
<thead>
<tr>
<th>Cisco Unified CME Version</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.0</td>
<td>Class of restriction was introduced for Cisco Unified CME.</td>
</tr>
</tbody>
</table>

Related Features

Ephone-dn Templates

The corlist command can be included in an ephone-dn template that is applied to one or more ephone-dns. For more information, see the “Ephone-dn Templates” section on page 322.
Distinctive Ringing Overview

Note

For a summary of the functionality introduced in different releases, see the “Feature History for Distinctive Ringing” section on page 504.

In Cisco Unified CME 4.0 and later versions, an extension can be set to distinguish internal calls, internal calls, and feature ringing. When the phone is ringing, the ring pattern will be distinctive and identify those types of calls. If the phone is already in use, an incoming call is presented as a call-waiting call using a distinctive call-waiting beep.

The `ring` command allows one of the three ring styles supported by SCCP to be selected - internal, external or feature ring. Regardless of which of these three styles of ring is selected, the call-waiting beep used for the call-waiting case always selects the distinctive call-waiting beep.

If the `primary` or `secondary` keyword is used, then the distinctive ring or beep is only selected if the incoming called number matches the primary number or secondary number defined for the ephone-dn. If there is no secondary number defined for the ephone-dn, then the secondary ring option has no effect.

Configuring Distinctive Ringing

This procedure sets up different ring patterns for internal calls, external calls, and feature notifications.

SUMMARY STEPS

1. enable
2. configure terminal
3. ephone-dn dn-tag [dual-line]
4. number number [secondary number] [no-reg [both | primary]]
5. ring {external | internal | feature} [primary | secondary]
6. exit
## DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> ephone-dn dn-tag [dual-line]</td>
<td>Enters ephone-dn configuration mode, creates an ephone-dn, and optionally assigns it dual-line status.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# ephone-dn 29</td>
<td></td>
</tr>
<tr>
<td></td>
<td>dn-tag — Unique sequence number that identifies this ephone-dn during configuration tasks. The maximum number of ephone-dns for a particular Cisco Unified CME system is version- and platform-specific. Refer to CLI help for the range of values.</td>
</tr>
<tr>
<td></td>
<td>dual-line— (Optional) Enables an ephone-dn with one voice port and two voice channels, which supports features such as call waiting, call transfer, and conferencing with a single ephone-dn.</td>
</tr>
<tr>
<td><strong>Step 4</strong> number number [secondary number] [no-reg {both</td>
<td>primary}]</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-ephone-dn)# number 2333</td>
<td>number— String of up to 16 digits that represents a telephone or extension number.</td>
</tr>
<tr>
<td></td>
<td>secondary— (Optional) Allows you to associate a second telephone number with an ephone-dn.</td>
</tr>
<tr>
<td></td>
<td>no-reg— (Optional) Specifies that this number should not register with the H.323 gatekeeper. Unless you specify one of the optional keywords (both or primary) after the no-reg keyword, only the secondary number is not registered.</td>
</tr>
<tr>
<td><strong>Step 5</strong> ring {external</td>
<td>internal</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-ephone-dn)# ring internal</td>
<td>external— Use distinctive ring for external calls.</td>
</tr>
<tr>
<td></td>
<td>internal— Use distinctive ring for internal calls.</td>
</tr>
<tr>
<td></td>
<td>feature— Use distinctive ring for feature calls.</td>
</tr>
<tr>
<td></td>
<td>primary— (Optional) Use distinctive ring on primary number only.</td>
</tr>
<tr>
<td></td>
<td>secondary— (Optional) Use distinctive ring on secondary number only.</td>
</tr>
<tr>
<td><strong>Step 6</strong> exit</td>
<td>Exits ephone-dn configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-ephone-dn)# exit</td>
<td></td>
</tr>
</tbody>
</table>
Verifying Distinctive Ringing

**Step 1** Use the `show running-config` command to verify your configuration. Distinctive ringing is listed in the ephone-dn portion of the output.

Router# show running-config
ephone-dn 1 dual-line
   ring feature secondary
   number 126 secondary 1261
description Cashier1
call-forward busy 500 secondary
call-forward noan 500 timeout 10

**Step 2** Use the `show telephony-service ephone-dn` command to display only ephone-dn configuration information.

Router# show telephony-service ephone-dn
ephone-dn 2
   number 5002
   huntstop
call-forward noan 5001 timeout 8

**Examples**

The following example sets distinctive ringing for internal calls on extension 2333.

ephone-dn 34
   number 2333
   ring internal

**Feature History for Distinctive Ringing**

<table>
<thead>
<tr>
<th>Cisco Unified CME Version</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.0</td>
<td>Distinctive Ringing was introduced.</td>
</tr>
</tbody>
</table>

**Do Not Disturb**

The Do Not Disturb (DND) feature allows you to set your phone to forward calls without ringing the phone. This section describes the following topics:

- Do Not Disturb Overview, page 505
- Configuring Do Not Disturb, page 505
- Verifying Do Not Disturb, page 506
- Examples, page 506
Do Not Disturb Overview

For a summary of the functionality introduced in different releases, see the “Feature History for Do Not Disturb” section on page 508.

Do-not-disturb (DND) service can be enabled using the DND soft key on Cisco Unified IP phones that support soft keys. When DND is enabled, incoming calls do not ring on the phone, but they do provide visual alerting and call information and can be answered if desired. A display message indicates that DND is in effect. If no-answer call forwarding is enabled, calls are forwarded.

When a local IP phone calls another local IP phone that is in the DND state, the message "Ring out DND" is displayed on the calling phone indicating that the target phone is in the DND state. Pressing DND during an incoming call diverts the call to a call-forward no-answer destination. If call-forward no-answer is not configured, the ringer is disabled.

You can use the DND soft key to switch on or off the DND functionality in all call states except connected. That is, you can enable or disable DND when an incoming call is ringing or when you are not connected to a call. You cannot enable or disable DND when you are connected to an incoming call.

For Cisco CME 3.2.1 and later versions, do not disturb (DND) can be blocked from phones with the feature-ring function, which is configured with the f keyword in the button command. A feature ring is a triple-pulse ring, a type of ring cadence in addition to internal call and external call ring cadences. For example, an internal call in the United States rings for 2 seconds on and 4 seconds off (single-pulse ring), and an external call rings for 0.4 seconds on, 0.2 seconds off, 0.4 seconds on, and 0.2 seconds off (double-pulse ring).

The triple-pulse ring is used as an audio identifier for phone users. For example, each salesperson in a sales department could have an IP phone with a button sharing the same set of ephone-dns with the sales staff and another button for their private line for preferred customers. To help a salesperson identify an incoming call to his or her private line, the private line can be configured with the feature-ring function.

The no dnd feature-ring command disables the DND function on feature-ring lines. If this command were used for the configuration in the above example, the salespeople could activate DND on their phones and still hear calls to their private lines.

Prerequisites

Call-forwarding no-answer must be set for a phone in order to use DND to forward calls. No other configuration is necessary for basic DND.

Configuring Do Not Disturb

The basic DND feature is available to phones by default. This procedure only sets a DND bypass for phones that have buttons that are configured for feature ringing.

SUMMARY STEPS

1. enable
2. configure terminal
3. ephone phone-tag
4. no dnd feature-ring
5. exit

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 1 enable     | Enables privileged EXEC mode.  
| Example:  
| Router> enable    | - Enter your password if prompted. |
| Step 2 configure terminal | Enters global configuration mode. |
| Example:  
| Router# configure terminal | |
| Step 1 ephone phone-tag | Enters ephone configuration mode.  
| Example:  
| Router(config)# ephone 10 | - phone-tag—Unique sequence number that identifies the ephone to be configured. |
| Step 2 no dnd feature-ring | Allows phone buttons configured with the feature-ring option to ring when their IP phones are in do-not-disturb (DND) mode. |
| Example:  
| Router(config-ephone)# no dnd feature-ring | |
| Step 3 exit | Exits ephone configuration mode. |
| Example:  
| Router(config-ephone)# exit | |

**Verifying Do Not Disturb**

Basic DND is available by default and no configuration is necessary. To verify DND bypass for phone buttons that are configured with the feature-ring option, use the **show running-config** command and review the ephone portion of the output.

```plaintext
Router# show running-config

ephone 1
mac-address 662F.91B1.BE0B
speed-dial 1 330 label "Office"
type 7960 addon 1 7914
no dnd feature-ring
button 1f40 2f41 3f42 4:30
```

**Examples**

For the following configuration example, when DND is activated on ephone 1 and ephone 2, button 1 will ring, but button 2 will not.
ephone-dn 1
number 1001

ephone-dn 2
number 1002

ephone-dn 10
number 1110
preference 0
no huntstop

ephone-dn 11
number 1111
preference 1

ephone 1
button 1f1
button 2o10.11
no dnd feature-ring

ephone 2
button 1f2
button 2o10.11
no dnd feature-ring

**Troubleshooting Do Not Disturb**

**Step 1**
The `show ephone dnd` command displays all phones that have DND enabled.

```
Router# show ephone dnd

ephone-1 Mac:0007.0EA6.353A TCP socket:[1] activeLine:0 REGISTERED
mediaActive:0 offhook:0 ringing:0 reset:0 reset_sent:0 paging 0 debug:0
IP:1.2.205.205 52486 Telecaster 7960 keepalive 2729 max_line 6 DnD
button 1: dn 11 number 60011 CH1 IDLE
```

**Step 2**
The `show ephone-hunt` command displays the ready/not-ready status of hunt group agents. “Logout 0” means that all instances of the extension are in ready status. “Logout 1” means that one instance of the extension is in not-ready status. For more information about using the DND soft key to control ready/not-ready status, see the “Agent Status Control” section on page 403.

```
Router# show ephone-hunt

list of numbers:
8001, aux-number A8000A100, # peers 2, logout 1 ...
8002, aux-number A8000A101, # peers 1, logout 0...
8003, aux-number A8000A102, # peers 1, logout 0...
```
Feature History for Do Not Disturb

<table>
<thead>
<tr>
<th>Cisco Unified CME Version</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.2</td>
<td>DND was introduced.</td>
</tr>
<tr>
<td>3.2.1</td>
<td>DND bypass for feature-ring phones was introduced.</td>
</tr>
</tbody>
</table>

Related Features

**Call Forwarding**
To use the DND soft key to forward calls, you must enable call-forwarding no-answer. For more information, see the “Call Forwarding” section on page 372.

**Soft-Key Display**
You can remove or change the position of the DND soft key. For more information, see the “Soft-Key Display” section on page 551.

**Feature Access Codes (FACs)**
DND can be activated and deactivated using a feature access code (FAC) instead of the DND soft key when standard or custom FACs are enabled. The following is the standard FAC for DND:

- `DND—**7`

For more information, see the “Feature Access Codes” section on page 325.

**Agent Status Control for Ephone Hunt Groups and Cisco Unified CME B-ACD**
Ephone hunt group agents can control their ready/not-ready status (their ability to receive calls) using the DND function or the HLog function of their phones. When they use the DND soft key, they do not receive calls on any extension on their phones. When they use the HLog soft key, they do not receive calls on hunt group extensions, but they do receive calls on other extensions. For more information on agent status control and the HLog function, see the “Ephone Hunt Groups” section on page 396.

Headset Auto-Answer

Feature allows you to specify the lines on individual phones that should automatically connect to incoming calls when the headset key is activated. This section describes the following topics:

- Headset Auto-Answer Overview, page 509
- Configuring Headset Auto-Answer, page 511
- Verifying Headset Auto-Answer, page 512
- Examples, page 512
- Troubleshooting Headset Auto-Answer, page 513
- Feature History for Headset Auto-Answer, page 513
Headset Auto-Answer Overview

Note

For a summary of the functionality introduced in different releases, see the “Feature History for Headset Auto-Answer” section on page 513.

Cisco Unified CME 4.0 and later versions offer headset auto-answer, which allows you to configure lines on specific phones to automatically connect to incoming calls. The phone cannot be busy with an active call and the headset key must be engaged to receive automatically answered calls. Incoming calls are automatically answered one by one on the phone as long as the headset light remains lit.

For each phone, you can specify one or more lines for headset auto-answer. Note that a line is similar to, but not exactly the same as, a button on the phone. A line represents a phone’s capability to make a call connection, so each button that can make a call connection becomes a line. (For example, unoccupied buttons or speed-dial buttons are not lines.) Note also that a line is not the same as an ephone-dn. A button with overlaid ephone-dns is only one line, even though it has several ephone-dns (extension numbers) associated with it. In most cases an ephone’s line numbers do match its button numbers, but in a few cases they do not. Figure 37 illustrates a comparison of line numbers and button numbers for different types of phone configurations.

Once a phone has been configured for headset auto-answer, the phone user needs to press the headset key to start auto-answer. The headset light is lit to indicate that auto-answer is active for the lines that have been so designated in the configuration. When the phone auto-answers a call, a zip tone is played to alert the phone user that a call is present. To stop auto-answer, the phone user presses the headset key again and the headset light goes out. At this time, the phone user can answer calls in a normal manner using the handset.
**Figure 37 When is a Line the Same as a Button?**

Most of the time, a line number is the same as the button number on which it appears. In this example, line 1 is button 1, line 2 is button 2, and line 3 is button 3.

But not always. In the following case, line 2 is button 3, because button 3 is the second button that has an ephone-dn to be connected to a phone call. Button 2 is unoccupied and cannot take calls.

In the following example, button 2 has three overlay ephone-dns (22, 23, and 24). Button 2 is defined as one line because only one of those ephone-dns can be connected to a call using this button at any one time.

An expansion, or rollover, line for overlaid ephone-dns also counts as one line. Button 2 in this example is also line 2.
Configuring Headset Auto-Answer

This procedure specifies the line numbers on individual phones for which headset auto-answer should be activated.

SUMMARY STEPS

1. enable
2. configure terminal
3. ephone phone-tag
4. headset auto-answer line line-number
5. exit

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> ephone phone-tag</td>
<td>Enters ephone configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# ephone 25</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> headset auto-answer line line-number</td>
<td>Specifies a line on an ephone that will be answered automatically when the headset button is depressed.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-ephone)# headset auto-answer line 1</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong> Repeat this command to add additional lines.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> exit</td>
<td>Exits ephone configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-ephone)# exit</td>
<td></td>
</tr>
</tbody>
</table>
Verifying Headset Auto-Answer

**Step 1** Use the `show running-config` command to verify your configuration. Headset auto-answer is listed in the ephone portion of the output.

```
Router# show running-config

ephone 1
   headset auto-answer line 1
   headset auto-answer line 2
   headset auto-answer line 3
   headset auto-answer line 4
   username "Front Desk"
   mac-address 011F.92B0.BE03
   speed-dial 1 3 30 label "Billing"
   type 7960 add 1 7914
   no dnd feature-ring
   keep-conference
   button 1f40 2f41 3f42 4:30
   button 5:405 7m20 8m21 9m22
   button 10m23 11m24 12m25 13m26
   button 14m499 15:1 16m31 17f498
   button 18s500
   night-service bell
```

**Step 2** Use the `show telephony-service ephone` command to display only the ephone configuration portion of the running configuration.

**Examples**

The following example enables headset auto-answer on ephone 3 for line 1 (button 1) and line 4 (button 4).

```
ephone 3
   button 1:2 2:4 3:6 4o21,22,23,24,25
   headset auto-answer line 1
   headset auto-answer line 4
```

The following example enables headset auto-answer on ephone 17 for line 2 (button 2), which has overlaid ephone-dns, and line 3 (button 3), which is an overlay rollover line.

```
ephone 17
   button 1:2 2o21,22,23,24,25 3x2
   headset auto-answer line 2
   headset auto-answer line 3
```

The following example enables headset auto-answer on ephone 25 for line 2 (button 3) and line 3 (button 5). In this case, the button numbers do not match the line numbers because buttons 2 and 4 are not used.

```
ephone 25
   button 1:2 3:4 5:6
   headset auto-answer line 2
   headset auto-answer line 3
```
Troubleshooting Headset Auto-Answer

Step 1 Make sure that you haven’t confused button number with line number. Review the explanation in the “Headset Auto-Answer Overview” section on page 509.

Feature History for Headset Auto-Answer

<table>
<thead>
<tr>
<th>Cisco Unified CME Version</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.0</td>
<td>Headset auto-answer was introduced.</td>
</tr>
</tbody>
</table>

Intercom

Intercom is a dedicated two-way audio path between two phones. This section describes the following topics:

- Intercom Overview, page 513
- Configuring Intercom, page 515
- Verifying Intercom, page 517
- Examples, page 518
- Feature History for Intercom, page 518
- Related Features, page 518

Intercom Overview

Note For a summary of the functionality introduced in different releases, see the “Feature History for Intercom” section on page 518.

Cisco Unified CME supports intercom functionality for one-way and press-to-answer voice connections using a dedicated pair of intercom ephone-dns on two phones that speed-dial each other.

When an intercom speed-dial button is pressed, a call is speed-dialed to the ephone-dn that is the other half of the dedicated pair. The called ephone-dn automatically answers the call in speakerphone mode with mute activated, which provides a one-way voice path from the initiator to the recipient. A beep is sounded when the call is auto-answered to alert the recipient to the incoming call. To respond to the intercom call and open a two-way voice path, the recipient deactivates the mute function by taking one of the following actions:

- On a multibutton phone, pressing the Mute button.
- On a Cisco Unified IP Phone 7910, lifting the handset.
In Cisco 3.2.1 and later releases, the **no-mute** keyword can be used with the `intercom` command to deactivate the speaker-mute function on intercom calls. For example, if phone user 1 makes an intercom call to phone user 2, both users hear each other upon connection when no-mute has been configured. The benefit is that people who receive intercom calls can be heard without having to disable the mute function. The disadvantage is that people who receive intercom calls will have their conversations and nearby background sounds heard the moment an intercom call to them is connected, regardless of whether they are ready to take a call or not.

Intercom lines cannot be used in shared-line configurations. If an ephone-dn is configured for intercom operation, it must be associated with one IP phone only. The intercom attribute causes an IP phone line (ephone-dn) to operate as an autodial line for outbound calls and as an autoanswer-with-mute line for inbound calls. **Figure 38** shows an intercom between a receptionist and a manager.

To prevent an unauthorized phone from dialing an intercom line (and creating a situation in which a phone automatically answers a non-intercom call), you can assign the intercom ephone-dn a dialing string with an alphabetic character. No one can dial the alphabetic character from a normal phone, but the phone at the other end of the intercom can be configured to dial the number that contains the alphabetic character through the Cisco Unified CME router. For example, the intercom ephone-dns in **Figure 38** have been assigned numbers with alphabetic characters so that no one but the receptionist can call the manager on his or her intercom line, and no one but the manager can call the receptionist on his or her intercom line.

---

**Note**

An intercom requires configuration of two ephone-dns, one each on a separate phone.

---

**Figure 38  Intercom**

1. The receptionist at phone 6 makes an intercom call to phone 7 by pressing button 2.

   Phone 6 - Receptionist
   Button 1 is extension 2345, a normal line.
   Button 2 is extension A5001, a dedicated intercom connection to intercom extension A5002 on phone 7.

2. Phone 7 beeps once and automatically answers in speakerphone mode with mute activated. The manager hears the receptionist's voice and deactivates the mute function to open a two-way voice path for a reply.

   Phone 7 - Manager
   Button 1 is extension 4578, a normal line.
   Button 2 is extension A5002, a dedicated intercom connection to intercom extension A5001 on phone 6.
Configuring Intercom

This procedure sets up a dedicated two-way intercom between two phones.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. ephone-dn dn-tag
4. number number
5. name name
6. intercom directory-number [barge-in | no-auto-answer] [label label] [no-mute]
7. exit
8. Repeat Step 3 through Step 7 for the second ephone-dn.
9. ephone phone-tag
10. button button-number:dn-tag [[button-number:dn-tag] ...]
11. restart
12. exit
13. Repeat Step 9 through Step 12 for the second ephone.

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> ephone-dn dn-tag</td>
<td>Enters ephone-dn configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# ephone-dn 11</td>
<td>• dn-tag—Unique sequence number that identifies this intercom ephone-dn during configuration tasks.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Do not use the dual-line keyword with this command. Intercom ephone-dns cannot be dual-line.</td>
</tr>
</tbody>
</table>
### Intercom

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 4</strong> number number</td>
<td>Assigns a valid intercom number.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-ephone-dn)# number A2345</td>
<td>- <em>number</em>—String that contains up to 16 characters. If this ephone-dn is an intercom ephone-dn, alphabetic characters can be included for security. One or more alphabetic characters in an intercom number ensures that the number can only be dialed from the one other intercom number that is programmed to dial this number. The number cannot be dialed from a normal phone if it contains an alphabetic character.</td>
</tr>
</tbody>
</table>

| **Step 5** name name | Sets a name to be associated with the ephone-dn. This name is used for caller-ID displays and also shows up in the local directory associated with the ephone-dn. |
| **Example:** Router(config-ephone-dn)# name intercom | |

| **Step 6** intercom directory-number [barge-in | no-auto-answer] [label label] [no-mute] | Defines the ephone-dn that is speed-dialed for the intercom feature when this line is used. |
| **Example:** Router(config-ephone-dn)# intercom A2346 label Security | - *directory-number*—Number to speed-dial for this intercom function. |
|  | - *barge-in*—(Optional) Specifies that an intercom call on this ephone-dn will force an existing call on the associated ephone into a call-hold state and allow the intercom call to be immediately answered. |
|  | - *no-auto-answer*—(Optional) Creates a connection for the IP phone line resembling private line automatic ringdown (PLAR). |
|  | - *label label*—(Optional) Defines a text label of up to 24 characters for the intercom ephone-dn. This label is used for caller-ID displays and directory lists. |
|  | - *no-mute*—(Optional) Disables the speakerphone mute function so that incoming intercom calls can immediately hear the party being called. |

| **Step 7** exit | Exits ephone-dn configuration mode. |
| **Example:** Router(config-ephone-dn)# exit | |

| **Step 8** Repeat Step 3 through Step 7 for the second ephone-dn. | The intercom feature requires configuration of separate ephone-dns at each end of the two-way voice path. |

| **Step 9** ephone phone-tag | Enters ephone configuration mode. |
| **Example:** Router(config)# ephone 24 | - *phone-tag*—Unique sequence number that identifies the ephone that is to receive the intercom ephone-dn. |
### Verifying Intercom

**Step 1** Use the `show running-config` command to display the running configuration. Ephone-dns used for intercoms are listed in the ephone-dn portion of the output, and phones with intercoms are listed in the ephone part of the output.

```plaintext
Router# show running-config

ephone-dn 18
  number 5001
  name "intercom"
  intercom 5002

ephone-dn 19
  name "intercom"
  number 5002
  intercom 5001

ephone 4
  button 1:2 2:18

ephone 5
  button 1:4 2:19
```

**Step 2** Use the `show telephony-service ephone-dn` and `show telephony-service ephone` commands to display only the configuration information for ephone-dns and ephones.

---

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 10</strong> <code>button button-number:dn-tag {[button-number:dn-tag]} ...</code></td>
<td>Assigns a button number to the intercom ephone-dn that you just defined. Use the colon separator (:) between the button number and the intercom ephone-dn tag to indicate a normal ring for the intercom line. For other keywords and arguments for this command, refer to the <em>Cisco Unified CallManager Express Command Reference</em>.</td>
</tr>
<tr>
<td><strong>Step 11</strong> <code>restart</code></td>
<td>Performs a fast reboot of this ephone. Does not contact the Dynamic Host Configuration Protocol (DHCP) or TFTP server for updated information.</td>
</tr>
<tr>
<td><strong>Step 12</strong> <code>exit</code></td>
<td>Exits ephone configuration mode.</td>
</tr>
<tr>
<td><strong>Step 13</strong> Repeat Step 9 through Step 12 for the second ephone.</td>
<td>The intercom feature requires configuration of an ephone at each end of the two-way voice path.</td>
</tr>
</tbody>
</table>
Examples

The following example shows an intercom between two Cisco Unified IP phones. In this example, ephone-dn 2 and ephone-dn 4 are normal extensions, while ephone-dn 18 and ephone-dn 19 are set as an intercom pair. Ephone-dn 18 is associated with line button 2 on Cisco Unified IP phone 4. Ephone-dn 19 is associated with line button 2 on Cisco Unified IP phone 5. The two ephone-dns provide a two-way intercom between the two Cisco Unified IP phones.

```plaintext
ephone-dn 2
  number 5333

ephone-dn 4
  number 5222

ephone-dn 18
  number 5001
  name "intercom"
  intercom 5002 barge-in

ephone-dn 19
  name "intercom"
  number 5002
  intercom 5001 barge-in

ephone 4
  button 1:2 2:18

ephone 5
  button 1:4 2:19
```

Feature History for Intercom

<table>
<thead>
<tr>
<th>Cisco Unified CME Version</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.0</td>
<td>Intercom was introduced.</td>
</tr>
<tr>
<td>3.2.1</td>
<td>The no-mute function was introduced.</td>
</tr>
</tbody>
</table>

Related Features

Paging

The paging feature sets up a one-way audio path to deliver information to a group of phones at one time. For more information, see the "Paging" section on page 342.
MWI Line Selection

MWI line selection allows you to choose the phone line that will be monitored for voice-mail messages and will light an indicator when messages are present. This section describes the following topics:

- MWI Line Selection Overview, page 519
- Configuring MWI Line Selection, page 519
- Verifying MWI Line Selection, page 520
- Examples, page 521
- Troubleshooting MWI Line Selection, page 522
- Feature History for MWI Line Selection, page 522
- Related Features, page 522

MWI Line Selection Overview

For a summary of the functionality introduced in different releases, see the “Feature History for MWI Line Selection” section on page 522.

Previously, the message waiting indicator (MWI) lamp on a phone could be associated only with the primary line of an ephone. In Cisco Unified CME 4.0 and later versions, you can designate a phone line other than the primary line to be associated with the MWI lamp. Lines other than the one associated with the MWI lamp will display an envelope icon when there is a message waiting.

Note that a logical phone “line” is not the same as a phone button. A button with one or more ephone-dns assigned to it is considered one line. A button with no ephone-dns assigned to it does not count as a line. For examples of line numbers in different phone configurations, see the “Examples” section on page 521.

Configuring MWI Line Selection

This procedure selects the phone line that will be monitored for voice-mail messages for an individual phone.

SUMMARY STEPS

1. enable
2. configure terminal
3. ephone phone-tag
4. mwi-line line-number
5. exit
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>enable</strong>&lt;br&gt; Enables privileged EXEC mode.&lt;br&gt;• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router&gt; enable</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>configure terminal</strong>&lt;br&gt; Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router# configure terminal</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>ephone phone-tag</strong>&lt;br&gt; Enters ephone configuration mode.&lt;br&gt;• <em>phone-tag</em>—Unique sequence number that identifies this ephone during configuration tasks.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config)# ephone 36</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><strong>mwi-line line-number</strong>&lt;br&gt; Selects a phone line to receive MWI treatment; when a message is waiting for the selected line, the message waiting indicator is activated.&lt;br&gt;• <em>line-number</em>—Ephone line number. Range is from 1 to 34. Default is 1.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-ephone)# mwi-line 3</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><strong>exit</strong>&lt;br&gt; Exits ephone configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-ephone)# exit</td>
</tr>
</tbody>
</table>

### Verifying MWI Line Selection

**Step 1** Use the **show running-config** command to verify your configuration. MWI Line Selection is listed in the ephone portion of the output.

```
Router# show running-config
ephone 18
button 1:20 2:21 3:22 4:23
mwi-line 2
```

**Step 2** Use the **show telephony-service ephone** command to display only ephone configuration information.
Examples

The following example enables MWI on ephone 18 for line 2 (button 2), which has overlaid ephone-dns. Only a message waiting for the first ephone-dn (2021) on this line will activate the MWI lamp. Button 4 is unused. The line numbers in this example are as follows:

- Line 1—Button 1—Extension 2020
- Line 2—Button 2—Extension 2021, 2022, 2023, 2024
- Line 3—Button 3—Extension 2021, 2022, 2023, 2024 (rollover line)
- Button 4—Unused
- Line 4—Button 5—Extension 2025

ephone-dn 20
tnumber 2020

ephone-dn 21
tnumber 2021

ephone-dn 22
tnumber 2022

ephone-dn 23
tnumber 2023

ephone-dn 24
tnumber 2024

ephone-dn 25
tnumber 2025

ephone 18
button 1:20 2o21,22,23,24,25 3x2 5:26
mwil-line 2

The following example enables MWI on ephone 17 for line 3 (extension 609). In this case, the button numbers do not match the line numbers because buttons 2 and 4 are not used. The line numbers in this example are as follows:

- Line 1—Button 1—Extension 607
- Button 2—Unused
- Line 2—Button 3—Extension 608
- Button 4—Unused
- Line 3—Button 5—Extension 609

ephone-dn 17
tnumber 607

ephone-dn 18
tnumber 608

ephone-dn 19
tnumber 609

ephone 25
button 1:17 3:18 5:19
mwil-line 3
Troubleshooting MWI Line Selection

**Step 1** Make sure you haven’t confused button number with line number. Review the explanation in the “Headset Auto-Answer Overview” section on page 509.

Feature History for MWI Line Selection

<table>
<thead>
<tr>
<th>Cisco Unified CME Version</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.0</td>
<td>MWI line selection was introduced.</td>
</tr>
</tbody>
</table>

Related Features

**Voice-Mail Integration**

For more information about integrating a Cisco Unified CME system with various types of voice-mail systems, see the “Voice-Mail Support” section on page 299.

On-Hook Dialing

On-hook dialing allows you to make calls by dialing the number before picking up the handset. This section describes the following topics:

- On-Hook Dialing Overview
- Feature History for On-Hook Dialing

On-Hook Dialing Overview

On-hook dialing allows you to enter dialed digits with the phone on hook and the handset still in its cradle. Digits appear in the phone display as they are dialed, and a Backspace soft key (<<) allows you to erase digits that are entered incorrectly. When you have finished entering the digits and want the phone to dial the number, use one of the following methods:

- Press a line button or the **Dial** soft key if you are using the speakerphone or a headset.
- Pick up the handset.

No configuration is required to activate this feature.
Feature History for On-Hook Dialing

<table>
<thead>
<tr>
<th>Cisco Unified CME Version</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>On-hook dialing was introduced.</td>
</tr>
</tbody>
</table>

Speed Dial

Several speed-dial features allow you to enable phone users to make calls by pressing buttons or dialing abbreviated numbers. This section describes the following topics:

- Speed Dial Overview, page 523
- Configuring Speed Dial, page 524
- Verifying Speed Dial, page 535
- Examples, page 535
- Troubleshooting Speed Dial, page 536
- Feature History for Speed Dial, page 537
- Related Features, page 537

Speed Dial Overview

**Note**

For a summary of the functionality introduced in different releases, see the “Feature History for Speed Dial” section on page 537.

Cisco Unified CME provides a number of mechanisms to implement speed dialing on IP and analog phones. Table 32 provides a summary and comparison of the different types of speed dial that are available in Cisco Unified CME systems.

<table>
<thead>
<tr>
<th>Type of Speed Dial</th>
<th>Availability of Numbers</th>
<th>Description</th>
<th>How Configured</th>
</tr>
</thead>
</table>
| Using a Monitor-Line Button for Speed Dial | Speed-dial entries are local to a specific IP phone.  
There can be up to the number of monitor lines on a phone | IP phone buttons that are configured as monitor lines can be used to speed-dial the line that is being monitored. | Monitor lines must be set up by administrators. |
| Configuring a Local Speed Dial Menu | Speed-dial entries are systemwide.  
There can be up to 32 numbers.                         | Users invoke entries from the Directories > Local Speed Dial menu on IP phones. | Numbers are set up by administrators using an XML file called speeddial.xml. |
| Configuring a Personal Speed Dial Menu | Speed-dial entries are local to a specific IP phone.  
There can be up to 24 numbers per phone.                  | Users invoke entries from the Directories > Local Services > Personal Speed Dials menu on IP phones. | Numbers are set up by administrators using the fastdial command in ephone configuration mode. |
Phone Features

Configuring Speed-Dial

Each of the types of speed dial has separate configuration steps, which are described in the following sections:

- Using a Monitor-Line Button for Speed Dial, page 524
- Configuring a Local Speed Dial Menu, page 525
- Configuring a Personal Speed Dial Menu, page 527
- Configuring Speed-Dial Buttons and Abbreviated Dialing, page 528
- Bulk-Loading Speed-Dial Numbers, page 532

Using a Monitor-Line Button for Speed Dial

For Cisco CME 3.2 and later versions, a monitor-line button can be used to speed-dial the monitor line’s number. A monitor line is a line that is shared by two people. Only one person can make and receive calls on the shared line at a time, while the other person, whose line is in monitor mode, is able to see that the

### Table 32 Types of Speed Dial Available in Cisco Unified CME

<table>
<thead>
<tr>
<th>Type of Speed Dial</th>
<th>Availability of Numbers</th>
<th>Description</th>
<th>How Configured</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring Speed-Dial Buttons and Abbreviated Dialing</td>
<td>There can be a total of up to 99 speed-dial codes per phone. A maximum of 33 codes can be local to a particular phone. The remainder are used for systemwide speed-dial codes. <strong>Note</strong> Entries from 34 to 99 are available only in Cisco IOS Release 12.3(11)XL, 12.3(14)T, and later releases.</td>
<td>For IP phones, the first entries that are set up occupy any unused line buttons and are invoked when a user presses one of these line buttons. Subsequent entries are invoked when a phone user dials the speed-dial code (tag) and the Abbr soft key. Analog phone users invoke speed dial by entering an asterisk and the code (tag) number of the desired entry.</td>
<td>Local speed-dial codes from 1 to 33 are defined by administrators using the <code>speed-dial</code> command in ephone mode. Systemwide codes from 1 to 99 are defined by administrators using the <code>directory-entry</code> command in telephony-service configuration mode. If the same code has been defined for both local and systemwide speed dial, the local definition takes precedence. To prevent this conflict, use only codes 34 through 99 for systemwide speed-dial numbers.</td>
</tr>
<tr>
<td>Bulk-Loading Speed-Dial Numbers</td>
<td>There can be up to ten text files containing lists of many speed-dial numbers that are loaded into flash, slot, or TFTP locations to be accessed by phone users. The ten files can hold a total of up to 10,000 numbers.</td>
<td>Phone users dial the following sequence: <code>prefix-code list-id index [extension-digits]</code></td>
<td>Files containing lists of numbers are created by the system administrator. The lists can be global or personal. File locations are specified using the <code>bulk-speed-dial list</code> command and prefixes are set using the <code>bulk-speed-dial prefix</code> command.</td>
</tr>
</tbody>
</table>
line is in use. Speed dialing is available when monitor lines’ lamps are off, indicating that the line is not in use. For example, an assistant who wants to talk with a manager can press an unlit monitor-line button to speed-dial the manager’s number.

A monitor-line lamp can be off or unlit only when its line is in the idle call state. The idle state occurs before a call is made and after a call has been completed. For all other call states, the monitor line lamp is on or lit.

The following example shows a monitor-line configuration. Extension 2311 is the manager’s line, and ephone 1 is the manager’s phone. The manager’s assistant monitors extension 2311 on button 2 of ephone 2. When the manager is on the line, the lamp is lit on the assistant’s phone. If the lamp is not lit, the assistant can speed-dial the manager by pressing button 2.

```
ephone-dn 11
   number 2311

ephone-dn 22
   number 2322

ephone 1
   button 1:11

ephone 2
   button 1:22 2m11
```

### Configuring a Local Speed Dial Menu

The local speed-dial feature provides a systemwide list of frequently called numbers that can be programmed by an administrator on all phones, up to a maximum of 32 entries. Local speed-dial numbers are available from the Directories button on a phone.

To define local speed-dial numbers, a system administrator first creates an XML file called speeddial.xml, similar to the example shown in the “speeddial.xml File Example” section on page 525. After the administrator places the speeddial.xml file in the Cisco Unified CME router’s flash memory, the local speed-dial menu appears when Local Speed Dial is selected from the Directories menu.

#### Prerequisites

- In any text editor, create a file called speeddial.xml in the Cisco-specified directory DTD format. Use the keywords and format shown in the “speeddial.xml File Example” section on page 525 to specify names and numbers for a local speed-dial list. For more information about Cisco DTD formats, refer to Cisco IP Phone Services Application Development Notes.

- Copy the file to the TFTP server application on the Cisco Unified CME router.

#### speeddial.xml File Example

```
<CiscoIPPhoneDirectory>
   <Title>Local Speed Dial</Title>
   <Prompt>Record 1 to 1 of 1 </Prompt>

   <DirectoryEntry>
      <Name>Security</Name>
      <Telephone>71111</Telephone>
   </DirectoryEntry>

   <DirectoryEntry>
      <Name>Marketing</Name>
      <Telephone>71234</Telephone>
   </DirectoryEntry>
</CiscoIPPhoneDirectory>
```
SUMMARY STEPS

1. copy tftp flash
2. configure terminal
3. ip http server
4. ip http path flash:

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> copy tftp flash</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router# copy tftp flash</td>
<td></td>
</tr>
<tr>
<td>Address or name of remote host []? 172.24.59.11</td>
<td></td>
</tr>
<tr>
<td>Source filename []? speeddial.xml</td>
<td></td>
</tr>
<tr>
<td>Destination filename [speeddial.xml]?</td>
<td></td>
</tr>
<tr>
<td>Accessing tftp://172.24.59.11/speeddial.xml...</td>
<td></td>
</tr>
<tr>
<td>Erase flash:before copying? [confirm]n</td>
<td></td>
</tr>
<tr>
<td>Loading speeddial.xml from 172.24.59.11 (via FastEthernet0/0):!</td>
<td></td>
</tr>
<tr>
<td>[OK - 329 bytes]</td>
<td></td>
</tr>
<tr>
<td>Verifying checksum... OK (0xF5DB)</td>
<td></td>
</tr>
<tr>
<td>329 bytes copied in 0.044 secs (7477 bytes/sec)</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> ip http server</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# ip http server</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> ip http path flash:</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# ip http path flash:</td>
<td></td>
</tr>
</tbody>
</table>
Configuring a Personal Speed Dial Menu

The personal speed-dial menu feature allows you to program up to 24 personal speed-dial numbers per IP phone. This feature is available only on Cisco Unified IP Phones 7940, 7960, 7960G, 7970G and 7971G-GE.

Personal speed-dial numbers appear as menu entries displayed from the Directories > Local Services > Personal Speed Dials option on the phone. Personal speed-dial entries are displayed in alphabetical order.

SUMMARY STEPS

1. ephone phone-tag
2. fastdial dial-tag number name name-string
3. exit

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> ephone phone-tag</td>
<td>Enters ephone configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# ephone 1</td>
<td>· phone-tag—Unique sequence number for the phone for which you want to program personal speed-dial numbers.</td>
</tr>
<tr>
<td><strong>Step 2</strong> fastdial dial-tag number name name-string</td>
<td>Creates an entry for a personal speed-dial number on this IP phone.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-ephone)# fastdial 1 5552 name Sales</td>
<td>· dial-tag—Unique identifier to identify this entry during configuration. Range is from 1 to 24.</td>
</tr>
<tr>
<td></td>
<td>· number—Telephone number or extension to be dialed.</td>
</tr>
<tr>
<td></td>
<td>· name name-string—Label to appear in the Personal Speed Dial menu, containing a string of up to 24 alphanumeric characters. Personal speed dial is handled through an XML request, so characters that have special meaning to HTTP, such as ampersand (&amp;), percent sign (%), semicolon (;), angle brackets (&lt; &gt;), and vertical bars (</td>
</tr>
<tr>
<td><strong>Step 3</strong> exit</td>
<td>Exits ephone configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-ephone)# exit</td>
<td></td>
</tr>
</tbody>
</table>
Configuring Speed-Dial Buttons and Abbreviated Dialing

In a Cisco Unified CME system, each phone can have up to 33 local speed-dial numbers (codes 1 through 33), up to 99 systemwide speed-dial numbers (codes 1 through 99), or a combination of the two. If you program both a local and a systemwide speed-dial number with the same code (tag number), the local number takes precedence. In most cases you will want to reserve codes 1 through 33 for local, per-phone speed-dial numbers and use codes 34 through 99 for systemwide speed-dial numbers so that there is no conflict.

On an IP phone, a speed-dial number can be on a speed-dial button or it can be an abbreviated code that is dialed from the keypad. On an analog phone, a speed-dial number can only be an abbreviated code.

Each speed-dial definition contains a speed-dial code (an identifier also known as a tag) and usually the full extension or telephone number that should be dialed when the code is used at the phone. However, local speed-dial entries on IP phone buttons can be defined without telephone numbers so that phone users can enter whatever numbers they want from the phone. Local speed-dial definitions can also be created with locked numbers that cannot be changed from the phone. Systemwide speed-dial definitions cannot be changed from the phone.

Using Speed-Dial Buttons and Abbreviated Dialing

Speed-dial buttons and abbreviated dialing are accessed in different ways from IP phones and from analog phones, as described in the following sections:

- **IP Phones**
- **Analog Phones**

**Note**

On-hook abbreviated dialing is limited to Cisco Unified IP Phones 7905G, 7912G, 7920G, 7970G, and 7971G-GE.

**IP Phones**

IP phone buttons that are not used for extensions are automatically populated with local speed-dial definitions when they exist for the phone on which the buttons appear. Speed-dial definitions are assigned to phone buttons in the order of their code (tag) numbers. For example, if you define speed-dial 1, it is assigned to the first phone button that is available. If you have used two buttons for extensions on this phone, speed-dial 1 is assigned to the third physical button. When you define speed-dial 2, it is assigned to the fourth physical button on the phone, and so on.

If more speed-dial definitions are created than are supported by the IP phone setup, the extra speed-dial definitions can be dialed from IP phones using the following procedure for abbreviated dialing:

1. Press the one- or two-digit speed-dial code (tag number) and the Abbr soft key. The phone dials the full telephone number associated with the speed-dial tag in speakerphone (hands-free) mode.
2. Pick up the handset or activate the headset to transition to handset mode.

Note that prior to Cisco IOS Releases 12.3(11)XL and 12.3(14)T, speed-dial entries that were in excess of the number of physical phone buttons available were ignored by IP phones.

**Analog Phones**

Analog phone users who use a Cisco ATA-186, Cisco ATA-188, or Cisco VG 224 to connect to a Cisco Unified CME system use a different method to access speed-dial numbers. To dial a speed-dial number from an analog phone, use the following procedure for abbreviated dialing:
Phone Features

Speed Dial

- Press the asterisk (*) key and the two-digit speed-dial code (tag number) of the desired speed-dial number. For instance, press *01 to speed-dial the number that has been programmed as speed-dial 1 on that ephone.

Note that prior to Cisco IOS Releases 12.3(11)XL and 12.3(14)T, analog phones were limited to nine speed-dial numbers.

The following tasks are contained in this section:
- Defining Speed-Dial Buttons and Abbreviated Dialing Codes from the Router CLI, page 529
- Changing Existing Speed-Dial Button Information from an IP Phone, page 531

Defining Speed-Dial Buttons and Abbreviated Dialing Codes from the Router CLI

Speed-dial definitions can be added or modified by an administrator from the Cisco Unified CME router CLI. Local speed dial numbers on IP phones can be locked so that they cannot be changed from the phone or they can be defined as empty so that the phone user can enter a number to be dialed. Changes that are made to speed-dial button definitions are saved into the router nonvolatile random-access memory (NVRAM) configuration after a timer-based delay.

A speed-dial definition consists of a unique identifier (speed-tag), a number to dial, and an optional label. Local speed-dial definitions are automatically assigned to any IP phone buttons that remain unused after all the assigned extensions have been associated with buttons. Definitions are assigned in the order of their speed-dial identifier (speed-tag) numbers. Note that these identifier numbers are not related to the physical button layout of the phone.

Note

The speed-dial command is used to enter speed-dial definitions that are local to a particular phone, and the directory entry command is used to enter systemwide speed-dial definitions. If the same identifier (tag) is used in a local definition and in a systemwide definition, the local definition takes precedence.

Restrictions

On-hook abbreviated dialing using the Abbr soft key is supported only on the following phone types:
- Cisco Unified IP Phone 7905G
- Cisco Unified IP Phone 7912G
- Cisco Unified IP Phone 7920G
- Cisco Unified IP Phone 7970G
- Cisco Unified IP Phone 7971G-GE

SUMMARY STEPS

1. ephone phone-tag
2. speed-dial speed-tag digit-string [label label-text]
3. Repeat Step 2 to make additional speed-dial definitions on this phone.
4. restart
5. exit
6. telephony-service
7. directory entry {directory-tag number name name | clear}
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong>&lt;br&gt;ephone phone-tag</td>
<td>Enters ephone configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong>&lt;br&gt;Router(config)# ephone 55</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong>&lt;br&gt;speed-dial speed-tag digit-string [label label-text]</td>
<td>Defines a unique speed-dial identifier, a digit string to dial, and an optional label to display next to the button.</td>
</tr>
<tr>
<td><strong>Example:</strong>&lt;br&gt;Router(config-ephone)# speed-dial 1 +5001 label &quot;Head Office&quot;</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Repeat <strong>Step 2</strong> to make additional speed-dial definitions on this phone.</td>
</tr>
<tr>
<td><strong>Step 4</strong>&lt;br&gt;restart</td>
<td>Performs a fast reboot of this ephone. Does not contact the DHCP or TFTP server for updated information.</td>
</tr>
<tr>
<td><strong>Example:</strong>&lt;br&gt;Router(config-ephone)# restart</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong>&lt;br&gt;exit</td>
<td>Exits ephone-dn configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong>&lt;br&gt;Router(config-ephone)# exit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong>&lt;br&gt;telephony-service</td>
<td>Enters telephony-service configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong>&lt;br&gt;Router(config)# telephony-service</td>
<td></td>
</tr>
</tbody>
</table>
Changing Existing Speed-Dial Button Information from an IP Phone

Once an administrator has created one or more unlocked speed-dial definitions that appear on buttons on an IP phone, a phone user can reprogram the buttons by using the following steps.

SUMMARY STEPS

1. Select an available phone line.
2. Press the pound key (#).
3. Press the speed-dial button that you want to program.
4. Enter the full telephone number to be dialed when the button is pressed.
5. Press the speed-dial button that you are programming a second time.
6. Hang up the receiver or press a new speed-dial button.

DETAILED STEPS

Step 1 Select an available phone line. Lift the handset, press the NewCall soft key, or press a button. Listen for the dial tone. Note that the Newcall soft key must not be disabled for the Cisco Unified IP Phone 7905G and the Cisco Unified IP Phone 7912G.

Step 2 Press the pound key (#).

Step 3 Press the speed-dial button that you want to program. A short beep confirms that you are starting to program this button.

Step 4 Enter the full telephone number to be dialed when the button is pressed. The digits are output to the phone display. When speed-dial numbers are entered on a Cisco Unified IP Phones 7940 and 7940G or Cisco Unified IP Phones 7960 and 7960G, the Backspace soft key (<<) is available to let you correct digits that were typed incorrectly. To remove a speed-dial number without replacing it with a new one, press the pound key (#).

Step 5 Press the speed-dial button that you are programming a second time to indicate that you have finished entering the speed-dial digits and to store the new speed-dial number.

Step 6 Hang up the receiver or press a new speed-dial button, and repeat the process.

Directory entry

```
Step 7 directory entry ((directory-tag number name name) | clear)

Example:
Router(config-telephony)# directory entry 45 8185550143 name Corp Acctg
```

Adds a systemwide directory and speed-dial definition.

- **directory-tag**—Digit string that provides a unique identifier for this entry. Range is from 1 to 99. Tags 1 through 33 can be overridden by tags with the same number that are configured using the **speed-dial** command.
- **number**—String of up to 32 digits that provides the full telephone number for this entry.
- **name name**—String of up to 24 characters that provides a name for this entry.
- **clear**—Removes all directory entries that were made with this command.
Bulk-Loading Speed-Dial Numbers

In Cisco Unified CME 4.0 and later versions, up to ten text files containing lists of many speed-dial numbers can be loaded into flash, slot, or TFTP locations to be accessed by phone users. The ten files can hold a total of up to 10,000 numbers. Each list holds numbers that are in an appropriate format for dialing from IP phones and SCCP-enabled analog phones.

Bulk Speed-Dial Lists

Up to ten bulk speed-dial lists can be created in the format that is explained in this section. These lists might be corporate directory lists, regional lists, or local lists, for example. The speed-dial numbers in these lists can be global (available to all phones) or personal (available to one or more specified phones). Each list receives a unique speed-dial list ID number (sd-id) between 0 and 9.

Speed-dial list ID numbers that are not used for global speed-dial lists are available to identify personal, custom lists that are associated with individual phones. Global speed-dial lists are enabled for all phones using the bulk-speed-dial list command in telephony-service configuration mode. Personal speed-dial lists are enabled for one or more individual phones using the same command in ephone configuration mode.

Speed-dial lists can be displayed using the show telephony-service bulk-speed-dial command.

Bulk speed-dial lists contain entries of speed-dial codes and the associated phone numbers to dial. Each entry in a speed-dial list must appear on a separate line. The fields in each entry are separated by commas (,). A line that begins with a semicolon (;) is treated as a comment. The format of each entry is shown in the following line.

\[\text{index, digits[, name][, private][, append-digit]}\]

Table 33 explains the fields in a speed-dial entry.

### Table 33: Bulk Speed-Dial List Format

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>index</td>
<td>Zero-filled number that uniquely identifies this index entry.</td>
</tr>
<tr>
<td>digits</td>
<td>Telephone number to dialed. Represents a fully qualified E.164 number. Use a comma (,) to represent a one-second pause.</td>
</tr>
<tr>
<td>name</td>
<td>(Optional) Alphanumeric string to identify a name, up to 30 characters.</td>
</tr>
<tr>
<td>private</td>
<td>(Optional) Enter yes to block the display of the dialed number.</td>
</tr>
<tr>
<td>append-digit</td>
<td>(Optional) Enter yes to allow additional digits to be appended to this number when dialed.</td>
</tr>
</tbody>
</table>

Phone User Access to Bulk Speed-Dial Lists

To dial a number that is stored in a bulk speed-dial list, a phone user enters the following access pattern from the phone’s keypad. The IP phone display shows the name associated with the index number and the dialed number.

\[\text{prefix-code list-id index [extension-digits]}\]

Table 34 explains each field in the phone-user access pattern.
Table 34  Phone User Access to Speed-Dial Lists

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>prefix-code</td>
<td>Bulk speed-dial access code that contains one or more characters. This code</td>
</tr>
<tr>
<td></td>
<td>can be changed in the configuration using the <strong>bulk-speed-dial prefix</strong> command. Default is # (pound sign).</td>
</tr>
<tr>
<td>list-id</td>
<td>Single digit from 0 to 9 that identifies the bulk speed-dial list that</td>
</tr>
<tr>
<td></td>
<td>contains the number to be dialed.</td>
</tr>
<tr>
<td>index</td>
<td>Two- to four-digit index number that identifies the number to be dialed.</td>
</tr>
<tr>
<td></td>
<td>Leading zeroes are required. For example, if the list contains 999 entries,</td>
</tr>
<tr>
<td></td>
<td>the index number of the first entry is 001.</td>
</tr>
<tr>
<td>extension-digits</td>
<td>(Optional) Additional digits to be added to the end of the number that is</td>
</tr>
<tr>
<td></td>
<td>speed-dialed. If additional digits are to be added, the <strong>append-digit</strong></td>
</tr>
<tr>
<td></td>
<td>field in the number’s entry must have been set to <strong>yes</strong> when the number</td>
</tr>
<tr>
<td></td>
<td>was added to a bulk speed-dial list.</td>
</tr>
</tbody>
</table>

Prerequisites

The bulk speed-dial text files containing the lists must be available in a location that is available to the Cisco Unified CME router: flash, slot, or TFTP location.

SUMMARY STEPS

1. enable
2. configure terminal
3. telephony-service
4. bulk-speed-dial list list-id location
5. bulk-speed-dial prefix prefix-code
6. exit
7. ephone phone-tag
8. bulk-speed-dial list list-id location
# Speed Dial

## Detailed Steps

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
- Enter your password if prompted. |
| **Step 2** configure terminal | Enters global configuration mode. |
| **Step 3** telephony-service | Enters telephony-service configuration mode. |
| **Step 4** bulk-speed-dial list list-id location | Identifies the location of a bulk speed-dial list.  
- `list-id`—Digit that identifies the list to be used. Range is from 0 to 9.  
- `location`—Location of the bulk speed-dial text file in URL format. Valid storage locations are TFTP, Slot 0/1, and Flash memory. |
| **Step 5** bulk-speed-dial prefix prefix-code | Sets the prefix code that phone users dial to access speed-dial numbers from a bulk speed-dial list.  
- `prefix-code`—One- or two-character access code for speed dial. Valid characters are digits from 0 to 9, asterisk (*), and pound sign (#). Default is #. |
| **Step 6** exit | Exits telephony-service configuration mode. |
| **Step 7** ephone phone-tag | Enters ephone configuration mode.  
- `phone-tag`—Unique sequence number that identifies this ephone during configuration tasks. |
| **Step 8** bulk-speed-dial list list-id location | Identifies the location of a bulk speed-dial list.  
- `list-id`—Digit that identifies the list to be used. Range is from 0 to 9.  
- `location`—Location of the bulk speed-dial text file in URL format. Valid storage locations are TFTP, Slot 0/1, and Flash memory. |

---

**Example**:

- **Step 1**: `Router> enable`
- **Step 2**: `Router# configure terminal`
- **Step 3**: `Router(config)# telephony-service`
- **Step 4**: `Router(config-telephony)# bulk-speed-dial list 6 flash:sd_dept_0_1_8.txt`
- **Step 5**: `Router(config-telephony)# bulk-speed-dial prefix #7`
- **Step 6**: `Router(config-telephony)# exit`
- **Step 7**: `Router(config-telephony)# ephone 25`
- **Step 8**: `Router(config-telephony)# bulk-speed-dial list 7 flash:lmi_sd_list_08_24_95.txt`
Verifying Speed Dial

**Step 1**  
Use the `show running-config` command to verify your configuration. Speed dial numbers are listed in the ephone portion of the output. Bulk speed-dial commands are listed in the telephony-service portion of the output.

```
Router# show running-config
ephone 1
description Store ACD 1
username "Shed1"
mac-address 022F.60C0.B224
speed-dial 1 330 label "Manager"
type 7960 addn 1 7914
no dnd feature-ring
keep-conference
button 1f40 2f41 3f42 4:30
button 5:40 7m20 8m21 9m22
button 10m23 11m24 12m25 13m26
button 14m499 15:1 16m31 17f498
button 18s500
night-service bell!
```

**Step 2**  
Use the `show telephony-service ephone` command to display only the ephone configuration information.

---

**Examples**

This section contains the following examples:

- Local Speed Dial Menu: Example, page 535
- Personal Speed Dial Menu: Example, page 535
- Speed-Dial Buttons and Abbreviated Dialing: Example, page 536
- Bulk-Loading Speed Dial: Example, page 536

**Local Speed Dial Menu: Example**

The following example enables the Cisco web browser and sets the HTTP path to flash memory so that the speeddial.xml file in flash memory is accessible to IP phones:

```
ip http server
ip http path flash:
```

**Personal Speed Dial Menu: Example**

The following example creates a directory of three personal speed-dial listings for one IP phone:

```
ephone 1
fastdial 1 5489 name Marketing
fastdial 2 12125550155 name NY Sales
fastdial 3 12135550112 name LA Sales
```
Speed-Dial Buttons and Abbreviated Dialing: Example

The following example defines two locked speed-dial numbers with labels to appear next to the speed-dial buttons on ephone 1. These speed-dial definitions are assigned to the next empty buttons after all extensions have been assigned. For instance, if two extensions are assigned on the Cisco Unified IP Phones 7960 and 7960G, these speed-dial definitions appear on the third and fourth buttons.

The example also defines two systemwide speed-dial numbers with the directory entry command. One is a local extension and the other is a ten-digit telephone number.

ephone 1
  mac-address 1234.5678.ABCD
  button 1:24 2:25
  speed-dial 1 +5002 label Receptionist
  speed-dial 2 +5001 label Security

telephony-service
  directory entry 34 5003 name Accounting
  directory entry 45 8185550143 name Corp Acctg

Bulk-Loading Speed Dial: Example

The following example changes the default bulk speed-dial prefix to #7 and enables global bulk speed-dial list number 6 for all phones. It also enables a personal bulk speed-dial list for ephone 25.

telephony-service
  bulk-speed-dial list 6 flash:sd_dept_01_l_87.txt
  bulk-speed-dial prefix #7

ephone-dn 3
  number 2555

ephone-dn 4
  number 2557

ephone 25
  button 1:3 2:4
  bulk-speed-dial list 7 flash:lmi_sd_list_08_24_95.txt

Troubleshooting Speed Dial

**Step 1** Use the `debug ephone detail` command to diagnose problems with speed-dial numbers. For more information, see the Cisco IOS Debug Command Reference.

**Step 2** Use the `show telephony-service bulk-speed-dial` command to display information about speed-dial lists.

```
Router# show telephony-service bulk-speed-dial summary

<table>
<thead>
<tr>
<th>List-id</th>
<th>Entries</th>
<th>Size</th>
<th>Reference</th>
<th>url</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>40</td>
<td>3840</td>
<td>Global</td>
<td>tftp://192.168.254.254/phonedirs/uut.csv</td>
</tr>
<tr>
<td>1</td>
<td>20</td>
<td>1920</td>
<td>Global</td>
<td>phoneBook.csv</td>
</tr>
<tr>
<td>8</td>
<td>15</td>
<td>1440</td>
<td>Global</td>
<td>tftp://192.168.254.254/phonedirs/big.txt</td>
</tr>
<tr>
<td>6</td>
<td>24879</td>
<td>2388384</td>
<td>ephone-2</td>
<td>tftp://192.168.254.254/phonedirs/big.txt1</td>
</tr>
<tr>
<td>7</td>
<td>20</td>
<td>1920</td>
<td>ephone-2</td>
<td>phoneBook.csv</td>
</tr>
<tr>
<td>6</td>
<td>24879</td>
<td>2388384</td>
<td>ephone-3</td>
<td>big.txt</td>
</tr>
<tr>
<td>7</td>
<td>20</td>
<td>1920</td>
<td>ephone-3</td>
<td>phoneBook.csv</td>
</tr>
</tbody>
</table>

4 Global List(s) 4 Local List(s)
```
Feature History for Speed Dial

<table>
<thead>
<tr>
<th>Cisco Unified CME Version</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>Speed dial using the <code>speed-dial</code> command was introduced.</td>
</tr>
</tbody>
</table>
| 3.0                      | - Personal speed-dial using the `fastdial` command was introduced.  
                          - The number of speed-dial definitions that can be created was increased from 4 to 33.  
                          - The ability to program speed-dial numbers at the phone was introduced.  
                          - The ability to lock speed-dial numbers was introduced. |
| 3.2.1                    | - Abbreviated dialing was introduced.  
                          - Support for up to 33 speed-dial numbers on analog phones was introduced. |
| 4.0                      | Bulk loading of speed-dial numbers was introduced. |

Related Features

DSS Call Transfer
Monitor-line button speed dial, also known as direct station select (DSS) transfer, allows you to use a monitored line button to speed-dial a call to that extension. When you want to allow consultation during DSS transfers, the `transfer-system` command must be configured with the `full-consult` and `dss` keywords. For more information, see the “Call Transfer” section on page 465.

Called-Name Display

In certain circumstances, the called-name display feature allows you to specify that incoming calls should display a called-party name rather than a called number. This section describes the following topics:

- Called-Name Display Overview, page 538
- Configuring Called-Name Display, page 539
- Verifying Called-Name Display, page 540
- Examples, page 540
- Troubleshooting Called-Name Display, page 544
- Feature History for Called-Name Display, page 544
- Related Features, page 545
Called-Name Display Overview

For a summary of the functionality introduced in different releases, see the “Feature History for Called-Name Display” section on page 544.

When phone agents answer calls for several different departments or people, it is often helpful for them to see a display of the name of the party that was called rather than the number that was called. For example, if order-entry agents are servicing three catalogs with individual 800 numbers configured in one overlay ephone-dn set, they need to know which catalog is being called to give the correct greeting, such as “Thank you for calling catalog N. May I take your order?” The called-name display feature allows you to specify either of the following types of names to be displayed:

- The directory name that is associated with a number using the directory entry command. (Available for overlaid ephone-dns and non-overlaid ephone-dns.) Up to 100 names can be specified with the directory entry command. The numbers associated with these directory names must contain at least one wildcard character. Called-name displays of directory names is specified using the service dnis dir-lookup command.

- The ephone-dn name that is associated with a number using the name command. (Available for overlaid ephone-dns only.) Called-name displays of ephone-dn names is specified using the service dnis overlay command.

When you specify called-name displays of ephone-dn names for overlaid ephone-dn sets, calls to the first ephone-dn display caller IDs. Calls to the remaining ephone-dns display ephone-dn names. The following example shows a configuration for three phones that use the same set of overlaid ephone-dns for each phone’s button 1.

```
telephony-service
  service dnis overlay

  ephone-dn 1
    number 18005550000
  ephone-dn 2
    name department1
    number 18005550001
  ephone-dn 3
    name department2
    number 18005550002

  ephone 1
    button 1o1,2,3

  ephone 2
    button 1o1,2,3

  ephone 3
    button 1o1,2,3
```

The default display for all three phones is the number of the first ephone-dn listed in the overlay set (18005550000). A call is made to the first ephone-dn (18005550000), and the caller ID (for example, 4085550123) is displayed on all three phones. The user for phone 1 answers the call. The caller ID (4085550123) remains displayed on phone 1, and the displays on phone 2 and phone 3 return to the default display (18005550000). A call to the next ephone-dn is made. The default display on phone 2 and phone 3 is replaced with the called ephone-dn’s name (18005550001).
Prerequisites

For the called-name display of directory names, the primary or secondary number of an ephone-dn must be defined using at least one wildcard character (period or .). If this feature is used with an ephone hunt group, the primary or secondary pilot number must be defined using at least one wildcard character and the phone numbers in the list command cannot contain wildcard characters.

Restrictions

For non-overlaid ephone-dns, the called name that is displayed can only be the directory name that was entered using the directory entry command. Called-name display of the names entered for ephone-dns using the name command is only available for overlaid ephone-dns.

Configuring Called-Name Display

This procedure sets a parameter in the configuration that instructs an IP phone that is capable of display to display the name of the party that was called rather than the number.

Note

If the service dnis dir-lookup and service dnis overlay commands are both used in one configuration, the service dnis dir-lookup command will take precedence.

SUMMARY STEPS

1. enable
2. configure terminal
3. telephony-service
4. service dnis dir-lookup
5. service dnis overlay
6. exit

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>
## Verifying Called-Name Display

**Step 1**
Use the `show running-config` command to verify your configuration. Called-name display is shown in the telephony-service part of the output.

```
Router# show running-config
telephony-service
service dnis overlay
```

### Examples

This section contains the following examples:

- [Called-Name Display Using Directory Name for an Overlaid Ephone-dn Set: Example](#)
- [Called-Name Display Using Directory Name for a Hunt Group with Overlaid Ephone-dns: Example](#)
- [Called-Name Display Using Directory Name for Non-Overlaid Ephone-dns: Example](#)
- [Called-Number Display Using Ephone-dn Name for Overlaid Ephone-dns: Example](#)
Called-Name Display Using Directory Name for an Overlaid Ephone-dn Set: Example

The following is an example of a configuration of overlaid ephone-dns that uses wildcards in the secondary numbers for the ephone-dns. The wildcards allow you to control the display according to the number that was dialed. The example is for a medical answering service with three IP phones that accept calls for nine doctors on one button. When a call to 5550001 rings on button 1 on ephone 1 through ephone 3, “doctor1” is displayed on all three ephones.

For more information about making directory entries, see the “Directories” section on page 315. For more information about overlaid ephone-dns, see the “Overlaid Ephone-dns” section on page 429.

```
telephony-service
   service dnis dir-lookup

   directory entry 1 5550001 name doctor1
   directory entry 2 5550002 name doctor2
   directory entry 3 5550003 name doctor3

   directory entry 4 5550010 name doctor4
   directory entry 5 5550011 name doctor5
   directory entry 6 5550012 name doctor6

   directory entry 7 5550020 name doctor7
   directory entry 8 5550021 name doctor8
   directory entry 9 5550022 name doctor9

   ephone-dn 1
      number 5500 secondary 555000.

   ephone-dn 2
      number 5501 secondary 555001.

   ephone-dn 3
      number 5502 secondary 555002.

   ephone 1
      button 101,2,3
      mac-address 1111.1111.1111

   ephone 2
      button 101,2,3
      mac-address 2222.2222.2222

   ephone 3
      button 101,2,3
      mac-address 3333.3333.3333
```

Called-Name Display Using Directory Name for a Hunt Group with Overlaid Ephone-dns: Example

The following example shows a hunt-group configuration for a medical answering service with two phones and four doctors. Each phone has two buttons, and each button is assigned two doctors’ numbers. When a patient calls 5550341, Cisco Unified CME matches the hunt-group pilot secondary number (555....), rings button 1 on one of the two phones, and displays “doctor1.”

For more information about hunt-group behavior, refer to the “Ephone Hunt Groups” section on page 396. Note that wildcards are used only in secondary numbers and cannot be used with primary numbers. For more information about making directory entries, see the “Directories” section on page 315. For more information about overlaid ephone-dns, see the “Overlaid Ephone-dns” section on page 429.

```
telephony-service
   service dnis dir-lookup
```
max-redirect 20
directory entry 1 5550341 name doctor1
directory entry 2 5550772 name doctor1
directory entry 3 5550263 name doctor3
directory entry 4 5550150 name doctor4

ephone-dn 1
    number 1001
ephone-dn 2
    number 1002
ephone-dn 3
    number 1003
ephone-dn 4
    number 104

ephone 1
    button 101,2
    button 2,3,4
    mac-address 1111.1111.1111

ephone 2
    button 101,2
    button 2,3,4
    mac-address 2222.2222.2222

ephone-hunt 1 peer
    pilot number 5100 secondary 555....
    list 1001, 1002, 1003, 1004
    final number 5556000
    hops 5
    preference 1
    timeout 20
    no-reg

Called-Name Display Using Directory Name for Non-Overlaid Ephone-dns: Example
The following is a configuration for three IP phones, each with two buttons. Button 1 receives calls from
doctor1, doctor2, and doctor3, and button 2 receives calls from doctor4, doctor5, and doctor6.

For more information about making directory entries, see the “Directories” section on page 315.

telephony-service
    service dnis dir-lookup
directory entry 1 5550001 name doctor1
directory entry 2 5550002 name doctor2
directory entry 3 5550003 name doctor3
directory entry 4 5550010 name doctor4
directory entry 5 5550011 name doctor5
directory entry 6 5550012 name doctor6

ephone-dn 1
    number 1001 secondary 555000.
ephone-dn 2
    number 1002 secondary 555001.

ephone 1
    button 1:1
    button 2:2
    mac-address 1111.1111.1111
Called-Name Display

Called-Number Display Using Ephone-dn Name for Overlaid Ephone-dns: Example

The following example shows three phones that have button 1 assigned to pick up three 800 numbers for three different catalogs.

The default display for all four phones is the number of the first ephone-dn listed in the overlay set (18005550000). A call is made to the first ephone-dn (18005550000), and the caller ID (for example, 4085550123) is displayed on all phones. The user for phone 1 answers the call. The caller ID (4085550123) remains displayed on phone 1, and the displays on phone 2 and phone 3 return to the default display (18005550000). A call to the second ephone-dn (18005550001) is made. The default display on phone 2 and phone 3 is replaced with the called ephone-dn’s name (catalog1) and number (18005550001).

For more information about overlaid ephone-dns, see the “Overlaid Ephone-dns” section on page 429.

```text
telephony-service
  service dnis overlay

ephone-dn 1
  number 18005550000

ephone-dn 2
  name catalog1
  number 18005550001

ephone-dn 3
  name catalog2
  number 18005550002

ephone-dn 4
  name catalog3
  number 18005550003

ephone 1
  button 1o1,2,3,4

ephone 2
  button 1o1,2,3,4

ephone 3
  button 1o1,2,3,4
```
Troubleshooting Called-Name Display

**Step 1** Use the `show telephony-service directory-entry` command to display current directory entries.

```
Router# show telephony-service directory-entry

directory entry 1 5550341 name doctor1
directory entry 2 5550772 name doctor1
directory entry 3 5550263 name doctor3
```

**Step 2** Use the `show telephony-service ephone-dn` command to verify that you have used at least one wildcard (period or .) in the ephone-dn primary or secondary number or to verify that you have entered a name for the number.

```
Router# show telephony-service ephone-dn

ephone-dn 2
  number 5002 secondary 200.
  name catalogN
  huntstop
call-forward noan 5001 timeout 8
```

**Step 3** Use the `show ephone overlay` command to verify the contents of overlaid ephone-dn sets.

```
Router# show ephone overlay

ephone-1 Mac:0007.0E5A.353A TCP socket:[1] activeLine:0 REGISTERED
  mediaActive:0 offhook:0 ringing:0 reset:0 reset_sent:0 paging 0 debug:0
  IP:10.2.225.205 52486 Telecaster 7960  keepalive 2771 max_line 6

button 1: dn 11 number 60011 CH1 IDLE  overlay
button 2: dn 17 number 60017 CH1 IDLE  overlay
button 3: dn 24 number 60024 CH1 IDLE  overlay
button 4: dn 30 number 60030 CH1 IDLE  overlay
button 5: dn 36 number 60036 CH1 IDLE  CH2 IDLE  overlay
button 6: dn 39 number 60039 CH1 IDLE  CH2 IDLE  overlay

overlay 1: 11(60011) 12(60012) 13(60013) 14(60014) 15(60015) 16(60016)
overlay 2: 17(60017) 18(60018) 19(60019) 20(60020) 21(60021) 22(60022)
overlay 3: 23(60023) 24(60024) 25(60025) 26(60026) 27(60027) 28(60028)
overlay 4: 29(60029) 30(60030) 31(60031) 32(60032) 33(60033) 34(60034)
overlay 5: 35(60035) 36(60036) 37(60037)
overlay 6: 38(60038) 39(60039) 40(60040)
```

Feature History for Called-Name Display

<table>
<thead>
<tr>
<th>Cisco Unified CME Version</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.2</td>
<td>Called-name display was introduced.</td>
</tr>
</tbody>
</table>
Related Features

Overlaid Ephone-dns
Overlaid ephone-dns are ephone-dns that share the same physical line button on an IP phone. Overlaid ephone-dns can be used to receive incoming calls and place outgoing calls, and they are frequently used with the called-name display feature. For more information, see the “Overlaid Ephone-dns” section on page 429.

Directory Names
The Cisco Unified CME system automatically creates a local phone directory according to the telephone numbers that are assigned during ephone-dn configuration. Additional entries to the local Cisco Unified CME directory can be made using the directory entry command. These names can be displayed using the called-name display feature. For more information, see the “Directories” section on page 315.

Ephone-dn Numbers and Names
For more information about the number and name commands that set the numbers and names for ephone-dns, see the Cisco Unified CallManager Express Command Reference.

Ephone-dn Labels
Ephone-dn labels are configurable text strings that can be displayed instead of extension numbers next to ephone-dn line buttons. This section describes the following topics:

- Ephone-dn Labels Overview, page 545
- Configuring Ephone-dn Labels, page 546
- Verifying Ephone-dn Labels, page 547
- Examples, page 547
- Feature History for Ephone-dn Labels, page 547

Ephone-dn Labels Overview

Note
For a summary of the functionality introduced in different releases, see the “Feature History for Ephone-dn Labels” section on page 547.

The Ephone-dn Labels feature controls the display adjacent to an ephone-dn line button. By default, an IP phone displays the extension number that is set using the number command under an ephone-dn. The label support feature allows you to enter a meaningful text string for each ephone-dn so that a phone user with multiple lines can select a line by name instead of by phone number, thus eliminating the need to consult in-house phone directories.
Configuring Ephone-dn Labels

This procedure specifies a text string to appear next to an ephone-dn line button instead of the extension number for that ephone-dn.

SUMMARY STEPS

1. ephone-dn  
dn-tag
2. label  
label-string
3. exit
4. ephone  
phone-tag
5. restart
6. exit

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**
ephone-dn  
dn-tag | Enters ephone-dn configuration mode.  
- *dn-tag*—Unique sequence number that identifies the ephone-dn to which the label is to be associated. |
| **Example:**
Router(config)# ephone-dn 1 |
| **Step 2**
label  
label-string | Creates a custom label that is displayed on the phone next to the line button that is associated with this ephone-dn. The custom label replaces the default label, which is the number that was assigned to this ephone-dn.  
- *label-string*—String of up to 30 alphanumeric characters that provides the label text. |
| **Example:**
Router(config-ephone-dn)# label user1 |
| **Step 3**
exit | Exits ephone-dn configuration mode. |
| **Example:**
Router(config-ephone-dn)# exit |
| **Step 4**
ephone  
phone-tag | Enters ephone configuration mode.  
- *phone-tag*—Unique identifier (sequence number) of the ephone on which you are defining the new label. |
| **Example:**
Router(config)# ephone 1 |
| **Step 5**
restart | Performs a fast reboot of this ephone. Does not contact the DHCP or TFTP server for updated information. |
| **Example:**
Router(config-ephone)# restart |
| **Step 6**
exit | Exits ephone configuration mode. |
| **Example:**
Router(config-ephone)# exit |
Verifying Ephone-dn Labels

Step 1 Use the `show running-config` command to verify your configuration. Ephone-dn descriptions are listed in the ephone-dn portion of the output.

```
Router# show running-config
ephone-dn 1 dual-line
  number 150 secondary 151
  label MyLine
call-forward busy 160
call-forward noan 160 timeout 10
huntstop channel
no huntstop
```

Examples

The following example creates text labels for two ephone-dns:

```
ephone-dn 1
  number 2001
  label Sales

ephone-dn 2
  number 2002
  label Engineering
```

Feature History for Ephone-dn Labels

<table>
<thead>
<tr>
<th>Cisco Unified CME Version</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.0</td>
<td>Ephone-dn labels were introduced.</td>
</tr>
</tbody>
</table>

Phone Header Bar Display

This feature allows you to customize the content of an IP phone header bar, which is the top line of the IP phone display. This section describes the following topics:

- Phone Header Bar Display Overview, page 548
- Configuring Phone Header Bar Display, page 548
- Verifying Phone Header Bar Display, page 550
- Examples, page 550
- Troubleshooting Phone Header Bar Display, page 550
- Feature History for Phone Header Bar Display, page 551
- Related Features, page 551
Phone Header Bar Display Overview

Note
For a summary of the functionality introduced in different releases, see the “Feature History for Phone Header Bar Display” section on page 551.

Normally the IP phone header bar, or top line, of a Cisco Unified IP Phones 7940 and 7940G or Cisco Unified IP Phones 7960 and 7960G replicates the text that appears next to the first line button. The header bar is shown in Figure 39. The header bar can, however, contain a user-definable message instead of the extension number. For example, the header bar can be used to display a name or the full E.164 number of the phone. If no description is specified, the header bar replicates the extension number that appears next to the first button on the phone.

Figure 39  Cisco Unified IP Phone Display

<table>
<thead>
<tr>
<th>13:09</th>
<th>06/08/01</th>
<th>3270</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title line</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Content lines</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Prompt and status area</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Softkey 1</td>
<td>Softkey 2</td>
<td>Softkey 3</td>
</tr>
</tbody>
</table>

Configuring Phone Header Bar Display

This procedure allows you to specify custom content to appear in the top line or header bar of an IP phone display.

SUMMARY STEPS

1. enable
2. configure terminal
3. ephone-dn dn-tag
4. description display-text
5. exit
6. ephone phone-tag
7. restart
8. exit
## DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 1 | enable | Enables privileged EXEC mode.  
- Enter your password if prompted. |
| **Example:** | Router> enable |
| Step 2 | configure terminal | Enters global configuration mode. |
| **Example:** | Router# configure terminal |
| Step 1 | ephone-dn dn-tag | Enters ephone-dn configuration mode.  
- *dn-tag*—The unique sequence number that identifies the ephone-dn for which the description should be in effect. |
| **Example:** | Router(config)# ephone-dn 55 |
| Step 2 | description display-text | Defines a description for the header bar of a display-capable IP phone on which this ephone-dn appears as the first line.  
- *display-text*—Alphanumeric character string, up to 40 characters. String is truncated to 14 characters in the display. |
| **Example:** | Router(config-ephone-dn)# description 408-555-0134 |
| Step 3 | exit | Exits ephone-dn configuration mode. |
| **Example:** | Router(config-ephone-dn)# exit |
| Step 4 | ephone phone-tag | Enters ephone configuration mode.  
- *phone-tag*—Unique sequence number of the ephone on which the new description will appear. |
| **Example:** | Router(config)# ephone 1 |
| Step 5 | restart | Performs a fast reboot of this ephone. Does not contact the DHCP or TFTP server for updated information. |
| **Example:** | Router(config-ephone)# restart |
| Step 6 | exit | Exits ephone configuration mode. |
| **Example:** | Router(config-ephone)# exit |
Verifying Phone Header Bar Display

Step 1
Use the `show running-config` command to verify your configuration. Ephone-dn descriptions are listed in the ephone-dn portion of the output.

```
Router# show running-config
ephone-dn 1 dual-line
    number 150 secondary 151
description 555-0150
call-forward busy 160
call-forward noan 160 timeout 10
huntstop channel
no huntstop
```

Examples

The following example provides the full E.164 number for a phone line in the phone header bar:

```
ephone-dn 55
    number 2149
description 408-555-0149
```

```
ephone-dn 56
    number 2150
```

ephone 12
button 1:55 2:56

Troubleshooting Phone Header Bar Display

Step 1
Use the `show telephony-service ephone` command to make sure that the ephone-dn to which you applied the description appears on the first button on the ephone. In the example below, ephone-dn 22 should have the description to appear in the phone display header bar.

```
Router# show telephony-service ephone
ephone 34
    mac-address 0030.94C3.F96A
    button 1:22 2:23 3:24
    speed-dial 1 5004
    speed-dial 2 5001
```
Feature History for Phone Header Bar Display

<table>
<thead>
<tr>
<th>Cisco Unified CME Version</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.01</td>
<td>Phone header bar display is introduced.</td>
</tr>
</tbody>
</table>

Related Features

Phone Display Messages
You can display a text message or HTML file in the display window of idle IP phones. For more information, see the “System Message Display” section on page 557.

Soft-Key Display

Soft-key display per phone allows you to customize the display and order of soft keys during the various call states for individual IP phones by using ephone templates. This section describes the following topics:

- Soft-Key Display Overview, page 551
- Configuring Soft-Key Display, page 553
- Verifying Soft-Key Display, page 555
- Examples, page 555
- Troubleshooting Soft-Key Display, page 556
- Feature History for Soft-Key Display, page 557
- Related Features, page 557

Soft-Key Display Overview

Note
For a summary of the functionality introduced in different releases, see the “Feature History for Soft-Key Display” section on page 557.

In each call state (alerting, connected, hold, idle, and seized), soft keys that are appropriate for the call state are displayed by default. Using ephone templates, you can delete soft keys that would normally appear or change the order in which the soft keys appear. For example, you might have one or more phones on which you do not want the Transfer soft key to appear. Or you might not want the NewCall soft key to appear during the hold state so that a phone user will not initiate a new call before concluding the call on hold. The call states are defined as follows:

- Alerting—When the remote point is being notified of an incoming call, and the status of the remote point is being relayed to the caller as either ringback or busy.
- Connected—When the connection to a remote point has been established.
- Hold—When a connected party is still connected but there is temporarily no voice connection.
Phone Features

Soft-Key Display

- Idle—Before a call is made and after a call is complete.
- Seized—When a caller is attempting a call but has not yet been connected.

Not all soft keys are available in all call states. Use CLI help to see the available soft keys for each call state. The soft keys are defined as follows:

- Acct—Short for “account code.” Provides access to configured accounts.
- Callback—Requests callback notification when a busy called line becomes free.
- CFwdALL—Short for “call forward all.” Forwards all calls.
- Confrn—Short for “conference.” Connects callers to a conference call.
- DND—Short for “do not disturb.” Enables the do-not-disturb features.
- EndCall—Ends the current call.
- GPickUp—Short for “group call pickup.” Selectively picks up calls coming into a phone number that is a member of a pickup group.
- Flash—Short for “hookflash.” Provides hookflash functionality for public switched telephone network (PSTN) services on calls connected to the PSTN via a foreign exchange office (FXO) port.
- HLog—Places the phone of an ephone-hunt group agent into not-ready status or, if the phone is in not-ready status, it places the phone into ready status.
- Hold—Places an active call on hold and resumes the call.
- Login—Provides personal identification number (PIN) access to restricted phone features.
- NewCall—Opens a line on a speakerphone to place a new call. Note that the NewCall soft key must not be disabled for the Cisco Unified IP Phone 7905G and the Cisco Unified IP Phone 7912G.
- Park—Places an active call on hold so it can be retrieved from another phone in the system.
- PickUp—Selectively picks up calls coming into another extension.
- Redial—Redials the last number dialed.
- Trnsfer—Short for “call transfer.” Transfers an active call to another extension.

Soft-key order is changed by defining an ephone template and applying the template to one or more ephones. You can create up to twenty ephone templates but you cannot apply more than one template to an ephone. If you try to apply a second ephone template to an ephone that already has an ephone-template applied to it, the second ephone-template will overwrite the first ephone template information, but the new information will only take affect after you use the restart command to reboot the phone. If you do not reboot the phone, the previously configured ephone-template will remain in effect.

Note

The third soft-key button selection on the Cisco Unified IP Phone 7905G and Cisco Unified IP Phone 7912G is reserved for the Message soft key. For these phones’ templates, the third soft-key defaults to the Message soft key. For example, the softkeys idle Redial Dnd Pickup Login Gpickup command configuration displays, in order, the Redial, DND, Message, PickUp, Login, and GPickUp soft keys.
Configuring Soft-Key Display

This procedure specifies in ephone templates the display and order of soft keys for different call states. The templates are then applied to individual phones.

**Note**
The HLog soft key must be enabled with the `hunt-group logout HLog` command before it will be displayed. For more information, see the “Ephone Hunt Groups” section on page 396. The Flash soft key must be enabled with the `fxo hook-flash` command before it will be displayed. For more information, see the “Flash Soft Key” section on page 561.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. ephone-template `template-tag`
4. softkeys alerting [Acct] [Callback] [Endcall]
5. softkeys connected [Acct] [Confrn] [Endcall] [Flash] [Hlog] [Hold] [Park] [Transfer]
6. softkeys hold [Newcall] [Resume]
7. softkeys idle [Cfwdall] [Dnd] [Gpickup] [Hlog] [Login] [Newcall] [Pickup] [Redial]
8. softkeys seized [Cfwdall] [Endcall] [Gpickup] [Hlog] [Pickup] [Redial]
9. exit
10. ephone `phone-tag`
11. ephone-template `template-tag`
12. restart
13. exit

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Enter your password if prompted.</td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> ephone-template <code>template-tag</code></td>
<td>Enters ephone-template configuration mode to create an ephone template.</td>
</tr>
<tr>
<td>Example:</td>
<td>template-tag—Unique identifier for the ephone template that is being created. Range is from 1 to 20.</td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
</tr>
<tr>
<td>------</td>
<td>-------------------</td>
</tr>
<tr>
<td>4</td>
<td>softkeys alerting [Acct] [Callback] [Endcall]</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Router(config-ephone-template)# softkeys alerting Callback Endcall</td>
</tr>
</tbody>
</table>
| 5    | softkeys connected [Acct] [Callback] [Endcall] [Flash] [Hlog] [Hold] [Park] [Transfer] | (Optional) Configures an ephone template for soft-key display during the call-connected stage. The default is that all keys are displayed in alphabetical order.  
- To display keys during the connected stage, enter any or all of the following keywords in any order: Acct, Callback, Endcall, Flash, Hlog, Hold, Park, Transfer.  
- Soft keys that are not explicitly defined will be disabled. |
|      | Example:          |         |
|      | Router(config-ephone-template)# softkeys connected Endcall Hold Transfer Hlog |         |
| 6    | softkeys hold [Newcall] [Resume] | (Optional) Configures an ephone template for soft-key display during the call-hold stage. The default is that the NewCall and Resume soft keys are displayed.  
- To display keys during call-hold, enter any or all of the following keywords in any order: Newcall, Resume.  
- Soft keys that are not explicitly defined will be disabled. |
|      | Example:          |         |
|      | Router(config-ephone-template)# softkeys hold Resume |         |
| 7    | softkeys idle [ Cfwdall] [Dnd] [Gpickup] [Hlog] [Login] [Newcall] [Pickup] [Redial] | (Optional) Configures an ephone template for soft-key display during the idle stage. The default is that all keys are displayed in alphabetical order.  
- To display keys during the idle stage, enter any or all of the following keywords in any order: Cfwdall, Dnd, Gpickup, Hlog, Login, Newcall, Pickup, Redial.  
- Soft keys that are not explicitly defined will be disabled. |
|      | Example:          |         |
|      | Router(config-ephone-template)# softkeys idle Newcall Redial Pickup Cfwdall Hlog |         |
| 8    | softkeys seized [ Cfwdall] [Endcall] [Gpickup] [Hlog] [Pickup] [Redial] | (Optional) Configures an ephone template for soft-key display during the seized stage. The default is that all keys are displayed in alphabetical order.  
- To display keys during the idle stage, enter any or all of the following keywords in any order: Cfwdall, Dnd, Gpickup, Hlog, Login, Newcall, Pickup, Redial.  
- Soft keys that are not explicitly defined will be disabled. |
|      | Example:          |         |
|      | Router(config-ephone-template)# softkeys seized Endcall Redial Pickup Cfwdall Hlog |         |
| 9    | exit               | Exits ephone-template configuration mode. |
|      | Example:          |         |
|      | Router(config-ephone-template)# exit |         |
| 10   | ephone phone-tag   | Enters ephone configuration mode.  
- *phone-tag*—Unique sequence number that identifies this ephone during configuration tasks. |
|      | Example:          |         |
|      | Router(config)# ephone 36 |         |
Verifying Soft-Key Display

**Step 1** Use the `show running-config` command to verify your configuration. The application of ephone templates to ephones is listed in the ephone portion of the output.

```
Router# show running-config

! 
ephone-dn 1 dual-line 	ring feature secondary
number 126 secondary 1261
description Sales
name Smith
call-forward busy 500 secondary
call-forward noan 500 timeout 8
huntstop channel
no huntstop
no forward local-calls
!
```

**Step 2** Use the `show telephony-service ephone-template` command to verify the contents of individual ephone templates.

```
Router# show telephony-service ephone-dn

ephone-dn 2
number 5002
huntstop
call-forward noan 5001 timeout 8
```

**Examples**

This section contains the following examples:

- **Modifying Soft Keys:** Example, page 556
- **Adding the HLog Soft Key for Ephone Hunt Groups:** Example, page 556

---

### Command or Action | Purpose
---|---
Step 11 **ephone-template** template-tag | Applies an ephone template to the ephone that is being configured.  
**Example:** Router(config-ephone)# ephone-template 15

Step 12 **restart** | Performs a fast reboot of this ephone. Does not contact the DHCP or TFTP server for updated information.  
**Note** You can restart all ephones using the **restart all** command in telephony-service configuration mode.

**Example:** Router(config-ephone)# restart

Step 13 **exit** | Exits ephone configuration mode.

**Example:** Router(config-ephone)# exit
Modifying Soft Keys: Example

The following example modifies soft-key display on four phones by creating two ephone templates. Ephone template 1 is applied to ephone 11, 13, and 15. Template 2 is applied to ephone 34. The soft-key displays on all other phones use the default arrangement of keys.

```plaintext
ephone-template 1
  softkeys idle Redial Newcall
  softkeys connected Endcall Hold Transfer

ephone-template 2
  softkeys idle Redial Newcall
  softkeys seized Redial Endcall Pickup
  softkeys alerting Redial Endcall
  softkeys connected Endcall Hold Transfer

ephone 10
  ephone-template 2

ephone 13
  ephone-template 1

ephone 15
  ephone-template 1

ephone 34
  ephone-template 2
```

Adding the HLog Soft Key for Ephone Hunt Groups: Example

The following example establishes the appearance and order of soft keys for phones that are configured with ephone-template 7. These phones will have the HLog key available when they are idle, when they have seized a line, or when they are connected to a call. Phones without soft keys can use the standard HLog codes to toggle ready and not-ready status.

```plaintext
  telephony-service
    hunt-group logout HLog
    fac standard

  ephone-template 7
    softkeys connected Endcall Hold Transfer Hlog
    softkeys idle Newcall Redial Pickup Cfwdall Hlog
    softkeys seized Endcall Redial Pickup Cfwdall Hlog
```

Troubleshooting Soft-Key Display

---

**Step 1**  Make sure that the templates have been properly applied to the phones on which you want to change the soft-key display.

**Step 2**  Make sure that you reset the phones after you apply the templates.
Feature History for Soft-Key Display

<table>
<thead>
<tr>
<th>Cisco Unified CME Version</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.2</td>
<td>Configurable soft-key display (the ability to customize soft-key display in the alerting, connected, idle, and seized call states) was introduced.</td>
</tr>
</tbody>
</table>
| 4.0 | • An optional HLog soft key was added to the connected, idle, and seized call states.  
• The ability to customize soft-key display in the hold call state was added. |

Related Features

Ephone Templates
The softkeys commands are included in ephone templates that are applied to one or more individual ephones. For more information about templates, see the “Ephone Templates” section on page 318.

HLog Soft Key
The HLog soft key must be enabled with the hunt-group logout HLog command before it will be displayed. For more information, see the “Ephone Hunt Groups” section on page 396.

Flash Soft Key
The Flash soft key must be enabled with the fxo hook-flash command before it will be displayed. For more information, see the “Flash Soft Key” section on page 561.

System Message Display

This feature allows you to specify a custom text or display message to appear in the lower portion of the display window on display-capable IP phones. This section describes the following topics:

- System Message Display Overview, page 558
- Configuring System Message Display, page 558
- Verifying System Message Display, page 559
- Examples, page 560
- Troubleshooting System Message Display, page 560
- Feature History for System Message Display, page 561
- Related Features, page 561
System Message Display Overview

Note

For a summary of the functionality introduced in different releases, see the “Feature History for System Message Display” section on page 561.

The system message display feature allows you to change the default system message. If no message is set, the default message “Cisco Unified CME” is displayed. You can set a plain-text message or a file to display using this feature. The file can include graphics.

When you specify a text message, the number of characters that can be displayed is not fixed because IP phones typically use a proportional (as opposed to fixed-width) font. There is room for approximately 30 alphanumeric characters.

The display message is refreshed with a new message after one of the following events occurs:

- Busy phone goes back on-hook.
- Idle phone receives a keepalive message.
- Phone is restarted.

The file-display feature allows you to specify a file to display on display-capable IP phones when they are not in use. You can use this feature to provide the phone display with a system message that is refreshed at configurable intervals, similar to the way that the text message feature provides a message. The difference between the two is that the system text message feature displays a single line of text at the bottom of the phone display, whereas the system display message feature can use the entire display area and contain graphic images.

Configuring System Message Display

This feature specifies a message or file to display instead of the default text message in the bottom line of the display window on display-capable IP phones.

SUMMARY STEPS

1. enable
2. configure terminal
3. telephony-service
4. system message text-message
5. url idle url idle-timeout seconds
6. exit
## DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** | **enable**  
**Example:**  
Router> enable  
Enables privileged EXEC mode.  
- Enter your password if prompted. |
| **Step 2** | **configure terminal**  
**Example:**  
Router# configure terminal  
Enters global configuration mode. |
| **Step 3** | **telephony-service**  
**Example:**  
Router(config)#  
Enters telephony-service configuration mode. |
| **Step 4** | **system message text-message**  
**Example:**  
Router(config-telephony)# system message ABC Company  
Defines a text message to display when a phone is idle.  
- **text-message**—Alphanumeric string to display. Display uses proportional-width font, so the number of characters that are displayed varies based on the width of the characters that are used. The maximum number of displayed characters is approximately 30. |
| **Step 5** | **url idle url idle-timeout seconds**  
**Example:**  
Defines the location of a file to display on phones that are not in use and specifies the interval between refreshes of the display, in seconds.  
- **url**—Any URL that conforms to RFC 2396.  
- **seconds**—Time interval between display refreshes, in seconds. Range is from 0 to 300. |
| **Step 6** | **exit**  
**Example:**  
Router(config-telephony)# exit  
Exits telephony-service configuration mode. |

### Verifying System Message Display

**Step 1**  
Use the **show running-config** command to verify your configuration. System message display is listed in the telephony-service portion of the output.

```
Router# show running-config

telephony-service
fxo hook-flash
load 7960-7940 P00307020300
load 7914 S00104000100
max-ephones 100
max-dn 500
ip source-address 10.153.13.121 port 2000
max-redirect 20
timeouts ringing 100
```
system message XYZ Company
voicemail 7189
max-conferences 8 gain -6
call-forward pattern .T
moh flash:music-on-hold.au
multicast moh 239.10.10.1 port 2000
web admin system name server1 password server1
dn-webedit
time-webedit
transfer-system full-consult
transfer-pattern 92......
transfer-pattern 91........
transfer-pattern 93.......
transfer-pattern 94.......
transfer-pattern 95.......
transfer-pattern 96.......
transfer-pattern 97.......
transfer-pattern 98.......
transfer-pattern 99.......
transfer-pattern .T
secondary-dialtone 9
create cnf-files version-stamp Jan 01 2002 00:00:00

Examples

This section contains the following examples:

- System Text Message Display: Example, page 560
- System File Display: Example, page 560

System Text Message Display: Example

The following example specifies text that should be displayed on IP phones when they are not being used:

telephony-service
  system message ABC Company

System File Display: Example

The following example specifies that a file called logo.htm should be displayed on IP phones when they are not being used:

telephony-service

Troubleshooting System Message Display

Step 1  Be sure that the HTTP server is enabled.
Feature History for System Message Display

<table>
<thead>
<tr>
<th>Cisco Unified CME Version</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1</td>
<td>System message display on idle phones using HTML files was introduced.</td>
</tr>
<tr>
<td>3.0</td>
<td>System message display on idle phones using text messages was introduced.</td>
</tr>
</tbody>
</table>

Related Features

Phone Header Bar Display Feature
To customize the top line of an IP phone display, use the phone header bar display feature. For more information, see the “Phone Header Bar Display” section on page 547.

Flash Soft Key

The Flash soft key provides hookflash functionality for calls made on FXO trunks. This section contains the following topics:

- Flash Soft Key Overview, page 561
- Configuring Flash Soft Key, page 562
- Verifying Flash Soft Key, page 563
- Examples, page 563
- Feature History for Flash Soft Key, page 563
- Related Features, page 563

Flash Soft Key Overview

Note
For a summary of the functionality introduced in different releases, see the “Feature History for Flash Soft Key” section on page 563.

Certain public switched telephone network (PSTN) services, such as three-way calling and call waiting, require hookflash intervention from a phone user. A soft key, labeled Flash, provides this functionality for phones that support soft-key display and that use foreign exchange office (FXO) lines attached to the Cisco Unified CME system. The Flash soft key is enabled using the `fxo hook-flash` command.

Once a Flash soft key has been enabled on an IP phone, it is available to provide hookflash functionality during all calls except for local IP-phone-to-IP-phone calls. Note that hookflash-controlled services can be activated only if they are supported by the PSTN connection that is involved in the call and that the availability of the Flash soft key does not guarantee that hookflash-based services are actually accessible to the phone user.
Configuring Flash Soft Key

This procedure enables the display of the Flash soft key on phones that support soft-key display.

SUMMARY STEPS

1. enable
2. configure terminal
3. telephony-service
4. fxo hook-flash
5. restart all
6. exit

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Router&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> telephony-service</td>
<td>Enters telephony-service configuration mode.</td>
</tr>
<tr>
<td>Example: Router(config)# telephony-service</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> fxo hook-flash</td>
<td>Enables the Flash soft key on phones that support soft-key display, on PSTN calls using an FXO port.</td>
</tr>
<tr>
<td>Example: Router(config-telephony)# fxo hook-flash</td>
<td>Note: The Flash soft key display is automatically disabled for local IP-phone-to-IP-phone calls.</td>
</tr>
<tr>
<td><strong>Step 5</strong> restart all</td>
<td>Performs a fast reboot of all phones associated with this Cisco Unified CME router. Does not contact the DHCP or TFTP server for updated information.</td>
</tr>
<tr>
<td>Example: Router(config-telephony)# restart all</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> exit</td>
<td>Exits telephony-service configuration mode.</td>
</tr>
<tr>
<td>Example: Router(config-telephony)# exit</td>
<td></td>
</tr>
</tbody>
</table>
Verifying Flash Soft Key

**Step 1** Use the `show running-config` command to display an entire configuration, including Flash soft key, which is listed in the telephony-service portion of the output.

```plaintext
Router# show running-config

telephony-service
  fxo hook-flash
  load 7960-7940 P00305000600
  load 7914 S00103020002
  max-ephones 100
  max-dn 500
  .
  .
  .
```

**Step 2** Use the `show telephony-service` command to show only the telephony-service portion of the configuration.

Examples

The following example enables the Flash soft key for phones that support soft-key display, for PSTN calls through an FXO voice port.

```plaintext
telephony-service
  fxo hook-flash
```

Feature History for Flash Soft Key

<table>
<thead>
<tr>
<th>Cisco Unified CME Version</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.0</td>
<td>The Flash soft key was introduced.</td>
</tr>
</tbody>
</table>

Related Features

**Soft Key Control**

To move or remove the Flash soft key on one or more phones, create and apply an ephone template that contains the appropriate `softkeys` commands. For more information, see the “Soft-Key Display” section on page 551.
PC Port Disable

PC Port Disable allows you to deactivate the PC port on individual ephones. This section contains the following topics:

- PC Port Disable Overview, page 564
- Configuring PC Port Disable, page 565
- Verifying PC Port Disable, page 567
- Examples, page 568
- Troubleshooting PC Port Disable, page 568
- Feature History for PC Port Disable, page 568
- Related Features, page 569

**PC Port Disable Overview**

**Note**

For a summary of the functionality introduced in different releases, see the “Feature History for PC Port Disable” section on page 568.

An IP phone has two ports. One is connected to the wall, and the other is available for a PC connection. The PC port is enabled by default, but can be disabled in the router configuration. You can disable PC ports on all phones or on individual phones.

To disable the PC port on some, but not all, phones, you must enable individual configuration files for ephones, which is a separate feature described in the “Configuration File Support” section on page 91. Then you create an ephone template that disables the PC port and apply that template only to certain phones. The setting that you use in the ephone template overrides the setting in telephony-service configuration.

After you use the `service phone` command in an ephone template to set the PC port value to 1 and regenerate the configuration file, the associated value in the XML vendorConfig section of the configuration file will be set as follows:

```xml
<vendorConfig>
  <pcPort>1</pcPort>
</vendorConfig>
```

**Prerequisites**

To disable the PC port on individual phones, per-phone configuration files must be created as described in the “Storing Configuration Files on an External TFTP Server and Creating Per-Phone Configuration Files” section on page 113.
Configuring PC Port Disable

This procedure deactivates the PC port on individual IP phones or globally.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. ephone-template *template-tag*
4. service phone pcPort [0 | 1]
5. exit
6. ephone *phone-tag*
7. ephone-template *template-tag*
8. exit
9. telephony-service
10. service phone pcPort [0 | 1]
11. create cnf-files
12. reset all
13. exit

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> ephone-template <em>template-tag</em></td>
<td>Enters ephone-template configuration mode to create an ephone template.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# ephone-template 9</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> service phone pcPort [0</td>
<td>Enables or disables the PC port on each IP phone to which this template is applied.</td>
</tr>
<tr>
<td>[1]</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-ephone-template)# service phone pcPort 1</td>
<td></td>
</tr>
</tbody>
</table>

**Note**  For individual phones, the ephone-template-mode setting for this command overrides the telephony-service-mode setting for this command.
## Phone Features

**Command or Action** | **Purpose**
--- | ---
**Step 5** | **exit**
| | Exits ephone-template configuration mode.
**Example:**
Router(config-ephone-template)# exit

**Step 6** | **ephone phone-tag**
| | Enters ephone configuration mode.
| | • *phone-tag*—Unique sequence number that identifies this ephone during configuration tasks.
**Example:**
Router(config)# ephone 24

**Step 7** | **ephone-template template-tag**
| | Applies an ephone-dn template to the ephone-dn that is being configured.
**Example:**
Router(config-ephone)# ephone-template 9

**Step 8** | **exit**
| | Exits ephone configuration mode.
**Example:**
Router(config-ephone)# exit

**Step 9** | **telephony-service**
| | Enters telephony-service configuration mode.
**Example:**
Router(config)# telephony-service

**Step 10** | **service phone pcPort [0 | 1]**
| | Enables or disables PC ports on all IP phones.
| | • 0—Enables PC ports.
| | • 1—Disables PC ports.
**Note** For individual phones, the ephone-template setting for this command overrides the telephony-service setting for this command.
**Example:**
Router(config-telephony)# service phone pcPort 0

**Step 11** | **create cnf-files**
| | Builds the XML configuration files that are required for IP phones. Use this command after you update configuration file parameters.
**Example:**
Router(config-telephony)# create cnf-files
### Command or Action

**Step 12**

```
reset {all [time-interval] | cancel | mac-address mac-address | sequence-all}
```

**Example:**

Router(config-telephony)# reset all

Performs a complete reboot of all phones or the phone with the specified MAC address, including contacting the DHCP and TFTP servers for the latest configuration information.

- **all**—Resets all phones associated with a Cisco Unified CME router. This keyword causes the router to pause 15 seconds between the reset start for each successive phone.
- **time-interval**—(Optional) Time interval, in seconds, between the start of each phone reset. Range is from 0 to 60. Default is 15.
- **cancel**—Interrupts a sequential reset cycle.
- **mac-address**—Resets the phone that has the specified MAC address.
- **sequence-all**—Resets all phones associated with this Cisco Unified CME router. This keyword causes the router to wait until one reset is complete before starting to reset the next phone. After the reset timeout of 4 minutes, the router stops waiting for the currently registering phone to complete registration and starts to reset the next phone.

**Note**

You can also reset one phone at a time using the `reset` command in ephone configuration mode.

**Step 13**

```
exit
```

**Example:**

Router(config-telephony)# exit

Exits telephony-service configuration mode.

### Verifying PC Port Disable

**Step 1**

Use the `show running-config` command to verify your configuration.

```
Router# show running-config

ephone-template 1
  service phone pcPort 1
  
  ephone 1
    ephone-template 1
    mac-address 0022.0314.4A26
    type 7970
    button 1:1

```

Cisco Unified CallManager Express System Administrator Guide
Examples

The following example disables the PC port on ephones 26 and 27. All other ephones have their PC ports enabled.

Router(config)# ephone-template 8
Router(config-ephone-template)# service phone pcPort 1
Router(config-ephone-template)# exit
Router(config)# ephone 26
Router(config-ephone)# ephone-template 8
Router(config-ephone)# exit
Router(config)# ephone 27
Router(config-ephone)# ephone-template 8
Router(config-ephone)# exit
Router(config)# telephony-service
Router(config-telephony)# service phone pcPort 0
Router(config-telephony)# create cnf-files
Router(config-telephony)# reset all

Troubleshooting PC Port Disable

Step 1 Make sure that the templates have been properly applied to the phones.
Step 2 Make sure that you use the create cnf-files command to regenerate configuration files and reset the phones after you apply the templates.
Step 3 Use the show telephony-service tftp-bindings command to display the configuration files that are associated with individual phones

show telephony-service tftp-bindings

tftp-server system:/its/SEPDEFAULT.cnf
  tftp-server system:/its/SEPDEFAULT.cnf alias SEPDefault.cnf
  tftp-server system:/its/XMLDefault.cnf.xml alias XMLDefault.cnf.xml
  tftp-server system:/its/XMLDefault.cnf.xml alias XMLDefault.cnf.xml
  tftp-server system:/its/XMLDefault7960.cnf.xml alias SEP00036B54BB15.cnf.xml
  tftp-server system:/its/germany/7960-font.xml alias German_Germany/7960-font.xml
  tftp-server system:/its/germany/7960-dictionary.xml alias German_Germany/7960-dictionary.xml
  tftp-server system:/its/germany/7960-tones.xml alias Germany/7960-tones.xml
  tftp-server system:/its/germany/SCCP-dictionary.xml alias Germany/SCCP-dictionary.xml
  tftp-server system:/its/germany/SCCP-dictionary.xml alias Germany/SCCP-dictionary.xml

Feature History for PC Port Disable

<table>
<thead>
<tr>
<th>Cisco Unified CME Version</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.0</td>
<td>PC port disable capability was introduced.</td>
</tr>
</tbody>
</table>
Related Features

Ephone Templates
The service ephone command can be added to an ephone template that is applied to one or more individual ephones. For more information about templates, see the “Ephone Templates” section on page 318.

Per-Phone Configuration Files
To disable the PC port on some, but not all, phones, you must enable individual configuration files for ephones. For more information, see the “Configuration File Support” section on page 91.

URL Provisioning for Customized Function Buttons

URL provisioning for customized function buttons allows you to specify alternative XML files to be used by the function buttons on IP phones. This section describes the following topics:

- URL Provisioning for Customized Function Buttons Overview, page 569
- Configuring URL Provisioning for Customized Function Buttons, page 570
- Verifying URL Provisioning for Customized Function Buttons, page 571
- Examples, page 572
- Troubleshooting URL Provisioning for Customized Function Buttons, page 572
- Feature History for URL Provisioning for Customized Function Buttons, page 572

URL Provisioning for Customized Function Buttons Overview

Note For a summary of the functionality introduced in different releases, see the “Feature History for URL Provisioning for Customized Function Buttons” section on page 572.

The Cisco Unified IP Phones 7940 and 7940G and the Cisco Unified IP Phones 7960 and 7960G have customized function buttons that show phone call status and activities on the display panels. These customized function buttons also invoke programmable noncall-related services. The four buttons—Services, Directories, Messages, and Information (the i button)—are linked to appropriate feature operations through programmable URLs. The fifth button—Settings—is managed entirely by the phone. Operation of these services is determined by the IP phone capabilities and the content of the referenced URL.

Specific URLs are provisioned on the Cisco Unified IP phone to populate these buttons. The URLs point to XML-based web pages formatted with XML tags that the Cisco Unified IP phone understands and uses. When you press a function button, the Cisco Unified IP phone uses the configured URL to access the appropriate XML web page for instructions. The web page sends instructions to the Cisco Unified IP phone to display information on the screen for you to navigate. You can select options and enter information by using soft keys and the scroll button.
Configuring URL Provisioning for Customized Function Buttons

This procedure specifies alternative URLs for one or more function buttons on IP phones.

SUMMARY STEPS

1. enable
2. configure terminal
3. telephony-service
4. url {directories | information | messages | services} url
5. reset all [time-interval]
6. exit

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3 telephony-service</td>
<td>Enters telephony-service configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)#</td>
<td></td>
</tr>
</tbody>
</table>
**URL Provisioning for Customized Function Buttons**

### Command or Action

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 4</strong></td>
<td>Provisions URLs for use by Cisco Unified IP phones. The four keywords (directory, information, messages, and services) correspond to the four function buttons on an IP phone: Directories, Information, Messages, and Services. The <code>url</code> command provisions the URLs through the SEPDEFAULT.cnf configuration file supplied by the Cisco Unified CME router to the Cisco Unified IP phones during phone registration. The maximum character length for an URL is 128. You must reset the Cisco Unified IP phones before the <code>url</code> command can take effect. By default, the router automatically uses the local directory service. Provisioning the directory URL to select an external directory resource disables the Cisco Unified CME local directory service. You can also disable the local directory by entering the <code>no service local-directory</code> command. To use a Cisco Unified CallManager directory as an external directory source for Cisco Unified CME phones, the Cisco Unified CallManager must be made aware of the phones. You must list the MAC addresses of the Cisco Unified CME phones in the Cisco Unified CallManager and reset the phones from the Cisco Unified CallManager. It is not necessary for you to assign ephone-dns to the phones or for the phones to register with Cisco Unified CallManager.</td>
</tr>
<tr>
<td>`url {directories</td>
<td>information</td>
</tr>
</tbody>
</table>

### Example:

**Step 5** resets all [time-interval] phones. Performs a complete reboot of all phones, including contacting the DHCP and TFTP servers for the latest configuration information.

**Example:**

Router(config-telephony)# reset all

- all—Resets all phones associated with the Cisco Unified CME router.
- time-interval—Time interval, in seconds, between the starts of successive phone resets. Range is 0 to 60. Default is 15.

**Step 6** exits telephony-service configuration mode.

**Example:**

Router(config-telephony)# exit

### Verifying URL Provisioning for Customized Function Buttons

**Step 1** Use the `show running-config` command to verify your configuration. URLs for customized function buttons are listed in the telephony-service portion of the output.

**Example:**

Router# show running-config

    telephony-service
    url information http://10.4.212.4/CCMUser/GetTelecasterHelpText.asp
Examples

The following example provisions the Information, Directories, Services, and Messages buttons.

```config
telephony-service
url information http://10.4.212.4/CCMUser/GetTelecasterHelpText.asp
url directories http://10.4.212.11/localdirectory
url services http://10.4.212.4/CCMUser/123456/urltest.html
url messages http://10.4.212.4/Voicemail/MessageSummary.asp
```

Troubleshooting URL Provisioning for Customized Function Buttons

**Step 1**  
Make sure the HTTP server is enabled and that there is communication between the Cisco Unified CME router and the server.

Feature History for URL Provisioning for Customized Function Buttons

<table>
<thead>
<tr>
<th>Cisco Unified CME Version</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.0</td>
<td>URL provisioning for customized function buttons was introduced.</td>
</tr>
</tbody>
</table>
SRST fallback support using Cisco Unified CME

This feature uses Cisco Unified CallManager Express (Cisco Unified CME) software on a gateway router to provide fallback support, also known as Survivable Remote Site Telephony (SRST), for Cisco Unified IP phones that are registered to a centralized Cisco Unified CallManager cluster attached to a Cisco router on your network. This document contains the following sections:

- SRST fallback support using Cisco Unified CME Overview, page 573
- Configuring SRST fallback support using Cisco Unified CME, page 578
- Examples, page 593
- Feature History for SRST Fallback Support Using Cisco Unified CME, page 594
- Related Features, page 594

Note: For more information about Cisco IOS voice features, see the entire Cisco IOS Voice Configuration Library—including library preface and glossary, feature documents, and troubleshooting information—at http://www.cisco.com/en/US/products/ps6441/prod_configuration_guide09186a0080565f8a.html.

SRST fallback support using Cisco Unified CME Overview

Note: For a summary of the functionality introduced in different releases, see the “Feature History for SRST Fallback Support Using Cisco Unified CME” section on page 594.

This feature enables routers to provide call-handling support for Cisco Unified IP phones when they lose connection to remote primary, secondary, or tertiary Cisco Unified CallManager installations or when the WAN connection is down. When SRST functionality is provided by Cisco Unified CME, provisioning of phones is automatic and most Cisco Unified CME features are available to the phones during periods of fallback, including hunt-groups, call park and access to Cisco Unity voice messaging services using SCCP protocol. The benefit of this solution is that Cisco Unified CallManager users will gain access to more features during fallback without any additional licensing costs.
SRST fallback service is still available to customers using Cisco Unified SRST, which offers a limited telephony feature set during fallback mode. Customers who require the following features should continue to use Cisco Unified Survivable Remote Site Telephony (SRST), as these features are not supported using Cisco Unified CME for SRST fallback service.

- More than 240 phones during fallback service
- Cisco VG 248 Analog Phone Gateway support
- Secure voice fallback during SRST fallback service
- Simple, one-time configuration for SRST fallback service

Cisco Unified CallManager supports Cisco Unified IP phones at remote sites attached to Cisco Integrated Services Routers across the WAN. SRST fallback support using Cisco Unified CME combines the many features available in Cisco Unified CME with the ability to automatically detect IP phone configurations that is available in Cisco Unified SRST to provide seamless call handling when communication with the Cisco Unified CallManager is interrupted.

When the system automatically detects a failure, SRST uses Simple Network Auto Provisioning (SNAP) technology to auto-configure a branch office router to provide call processing for the Cisco Unified IP phones that are registered with the router. When the WAN link or connection to the primary Cisco Unified CallManager is restored, call handling returns to the primary Cisco Unified CallManager.

A limited number of phone features are automatically detected at the time that call processing falls back to the Cisco Unified CME router in SRST mode, but an advantage of the SRST fallback support using Cisco Unified CME feature is that you can choose to prebuild a Cisco Unified CME configuration that contains a number of extensions (ephone-dns) with additional features that you want them to have. Prebuilt number and feature configurations for some or all of your extensions can contain features such as call forwarding, pickup groups, ephone hunt groups, soft-key templates, call park, class of restriction (COR), paging, night service, and access to local Cisco Unity ports. The configurations will contain ephone-dn configurations but will not identify which phones (which MAC addresses) will be associated with which ephone-dns (extension numbers).

By copying and pasting a prebuilt configuration onto Cisco Unified CME routers at several locations, you can use the same overall configuration for sites that are identically laid out. For example, if you have a number of retail stores, each with five to ten checkout registers, you can use the same overall configuration in each store. You might use a range of extensions from 1101 to 1110. Stores with fewer than ten registers will simply not use some of the ephone-dn entries you provide in the configuration. Stores with more extensions than you have prebuilt will use the auto-provisioning feature to populate their extra phones. The only configuration variations from store to store will be the specific MAC addresses of the individual phones, which are added to the configurations at the time of fallback.

When a phone registers for SRST service with a Cisco Unified CME router and the router discovers that the phone was configured with a specific extension number, the router searches for an existing prebuilt ephone-dn with that extension number and then assigns that ephone-dn number to the phone. If there is no prebuilt ephone-dn with that extension number, the Cisco Unified CME system automatically creates one. In this way, extensions without prebuilt configurations are automatically populated with extension numbers and features as the numbers and features are “learned” by the Cisco Unified CME router in SRST mode when the phone registers to the router after a WAN link fails.

The SRST fallback support using Cisco Unified CME feature is able to interrogate phones to learn their MAC addresses and the extension-to-ephone relationships associated with each phone. This information is used to dynamically create and execute the Cisco Unified CME button command for each phone and automatically provision each phone with the extensions and features you want it to have.
The following sequence describes how Cisco Unified CME provides SRST services for Cisco Unified CallManager phones when they lose connectivity with the Cisco Unified CallManager and fall back to the Cisco CME-SRST router:

**Before Fallback**

1. Phones are configured as usual in Cisco Unified CallManager.
2. The IP address of the Cisco Unified CME router is registered as the SRST reference on the Cisco Unified CallManager device pool.
3. SRST mode is enabled on the Cisco Unified CME router.
4. (Optional) Ephone-dns and features are prebuilt on the Cisco Unified CME router.

**During Fallback**

5. Phones that have been enabled for fallback register to the default Cisco Unified CME router that has SRST mode enabled. Each display-enabled IP phone displays the message that has been defined using the `system message` command under telephony-service configuration mode. By default, this message is “Cisco Unified CME.”
6. While the fallback phones are registering, the router in SRST mode initiates an interrogation of the phones in order to learn their phone and extension configurations. The following information is acquired or “learned” by the router:
   - MAC address
   - Number of lines or buttons
   - Ephone-dn-to-button relationship
   - Speed-dial numbers
7. Phones are registered as “virtual” phones and will appear in the output of a `show running-config` command that is run during the fallback period.
8. Based on the option chosen with the `srst mode` command, the Cisco CME-SRST router either saves or does not save the learned phone and extension information. If the information is saved, it appears in the output when you use the `show running-config` command and is saved to NVRAM when you use the `write` command.
9. While in fallback mode, Cisco Unified IP phones periodically attempt to reestablish a connection with Cisco Unified CallManager at the central office. Generally the default time that Cisco Unified IP phones wait before attempting to reestablish a connection to a remote Cisco Unified CallManager is 120 seconds. The time can be changed in Cisco Unified CallManager; see the “Device Pool Configuration Settings” chapter in the *Cisco Unified CallManager Administration Guide*. A manual phone reboot can immediately reconnect Cisco Unified IP phones to Cisco Unified CallManager.
10. Once a connection is reestablished with Cisco Unified CallManager, Cisco Unified IP phones automatically cancel their registration with the Cisco Unified CME router in SRST mode. However, if a WAN link is unstable, Cisco Unified IP phones can bounce between Cisco Unified CallManager and the Cisco Unified CME router in SRST mode.

An IP phone connected to SRST over a WAN reconnects itself to Cisco CallManager as soon as it can establish a connection with Cisco CallManager over the WAN link. However, if the WAN link is unstable, the IP phone switches back and forth between SRST and Cisco CallManager, causing temporary loss of phone service (no dial tone). These reconnect attempts, known as WAN link flapping issues, continue until the IP phone successfully reconnects itself back to Cisco CallManager.

WAN link disruptions can be classified into two types: infrequent random outages that occur on an otherwise stable WAN, and sporadic, frequent disruptions that last a few minutes.
To resolve WAN-link flapping issues between Cisco Unified CallManager and SRST, Cisco Unified CallManager provides an enterprise parameter and a setting in the Device Pool Configuration window called Connection Monitor Duration. (Depending upon system requirements, the administrator decides which parameter to use.) The value of the parameter is delivered to the IP phone in the XML configuration file.

- Use the enterprise parameter to change the connection duration monitor value for all IP phones in the Cisco Unified CallManager cluster. The default for the enterprise parameter is 120 seconds.
- Use the Device Pool Configuration window to change the connection duration monitor value for all IP phones in a specific device pool.

A Cisco Unified IP phone will not reestablish a connection with the primary Cisco Unified CallManager at the central office if it is currently engaged in an active call.

**After the FirstFallback**

11. If learned phone and extension information has been saved, it can now be used to set up additional features such as ephone hunt groups, which can contain learned extensions as well as prebuilt extensions. The complete core set of Cisco Unified CME phone features is available to the IP phones and extensions, whether they are learned or configured.

**Figure 40** shows a branch office with several Cisco Unified IP phones connected to a Cisco Unified CME router in SRST mode. The router provides connections to both a WAN link and the PSTN. The Cisco Unified IP phones connect to their primary Cisco Unified CallManager at the central office via this WAN link. **Figure 41** shows the interruption in service to Cisco Unified CallManager.
Prerequisites

- The IP address of the Cisco Unified CME router must be registered as the SRST reference on the Cisco Unified CallManager device pool.
- Cisco Unified CME 4.0 or a later version must be installed on the Cisco Unified CME router that is configured in SRST mode.
- The tasks described in the “Task 5: Setting Cisco Unified CME Parameters” section on page 60 must be completed. They include the following:
  - Providing TFTP access to phone firmware files and loading the files.
  - Specifying the maximum number of ephones and ephone-dns.
  - Specifying the Cisco Unified CME router IP address and port for phone registration.
  - Building the configuration file using the `create cnf-file` command.
  - Using the `transfer-system` command to specify full-blind or full-consult as the transfer method.

Restrictions

- The `call-manager-fallback` command, which is used to configure Cisco Unified SRST, cannot be used on a router that is configured for Cisco Unified CME.
- The number of phones that fall back to a Cisco Unified CME router in SRST mode cannot exceed the maximum number of phones that is supported by the router chassis. To find the maximum number of phones for a particular router and Cisco Unified CME version, see the Cisco Unified CallManager Express Supported Firmware, Platforms, Memory, and Voice Products document for that version. Links to this document are available in the Cisco Unified CME Documentation Roadmap.
• The ephone-dns and ephones that are created from fallback may have less information associated with them than appears in their original configuration on a Cisco Unified CallManager or on an active Cisco Unified CME system. This situation occurs because the Cisco Unified CME router in SRST mode is designed to learn only a limited amount of information from the fallback IP phones. For example, if an ephone-dn has in its configuration the command `number 4888 no-reg` (to keep that extension from registering under its E.164 address), after fallback the `no-reg` part of this command will be lost because this information cannot be learned from the IP phones.

• The order of the SRST fallback ephone-dns and ephones will be different from the order of the active Cisco Unified CallManager or Cisco Unified CME ephone-dns and ephones. For example, ephone 1 on an active Cisco Unified CallManager might be numbered ephone 5 on the Cisco Unified CME router in SRST mode, because the order of learned ephone-dns and ephones is determined by the sequence of the ephone fallback occurrence, which is purely random.

Configuring SRST fallback support using Cisco Unified CME

The configuration process is twofold: you enable SRST mode on the Cisco Unified CME router and you create ephone-dn configurations. The second procedure is optional if you need only limited phone functionality, because the system is able to learn basic configuration information about ephone-dns on its own.

• Specifying SRST Mode, page 578 (Required)
• Prebuilding Cisco Unified CME Ephone-dn Configurations, page 582 (Optional)

Specifying SRST Mode

This task sets a Cisco Unified CME router in SRST mode and specifies options to be used during fallback.

SUMMARY STEPS

1. enable
2. configure terminal
3. telephony-service
4. srst mode auto-provision {all | dn | none}
5. srst dn line-mode {dual | single}
6. srst dn template template-tag
7. srst ephone template template-tag
8. srst ephone description string
9. exit
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| 1    | enable            | Enables privileged EXEC mode.  
- Enter your password if prompted.  |
|      | **Example:**      |         |
|      | Router> enable    |         |
| 2    | configure terminal| Enters global configuration mode.  |
|      | **Example:**      |         |
|      | Router# configure terminal |         |
| 3    | telephony-service | Enters telephony-service configuration mode.  |
|      | **Example:**      |         |
|      | Router(config)# telephony-service |         |
| 4    | srst mode auto-provision {all | dn | none} | Enables SRST mode for a Cisco Unified CME router.  
- **all**—Include information for learned ephones and ephone-dns in the running configuration.  
- **dn**—Include information for learned ephone-dns in the running configuration.  
- **none**—Do not include information for learned ephones or learned ephone-dns in the running configuration.  |
|      | **Example:**      |         |
|      | Router(config-telephony)# srst mode auto-provision all |         |
| 5    | srst dn line-mode {dual | single} | (Optional) Specifies the line mode for ephone-dns in SRST mode on a Cisco Unified CME router.  
- **dual**—SRST fallback ephone-dns will be dual-line ephone-dns.  
- **single**—SRST fallback ephone-dns will be single-line ephone-dns.  
|      | **Note**          | This command is used only when ephone-dns are learned at the time of fallback. It is ignored when you prebuild ephone-dn configurations. |
|      | **Example:**      |         |
|      | Router(config-telephony)# srst dn line-mode dual |         |
| 6    | srst dn template template-tag | (Optional) Specifies an ephone-dn template to be used in SRST mode on a Cisco Unified CME router.  
- **template-tag**—Identifying number of an existing ephone-dn template. Range is from 1 to 15.  |
|      | **Example:**      |         |
|      | Router(config-telephony)# srst dn template 3 |         |
| 7    | srst ephone template template-tag | (Optional) Specifies an ephone template to be used in SRST mode on a Cisco Unified CME router.  
- **template-tag**—Identifying number of an existing ephone template. Range is from 1 to 20.  |
|      | **Example:**      |         |
|      | Router(config-telephony)# srst ephone template 5 |         |
Verifying SRST Mode

Step 1  
Use the `show telephony-service all` or the `show running-config` command to verify that SRST mode has been set on this router.

```
telephony-service
srst mode auto-provision all
srst ephone template 5
srst ephone description srst fallback auto-provision phone : Jul 07 2005 17:45:08
srst dn template 8
srst dn line-mode dual
load 7960-7940 P00305000600
max-ephones 30
max-dn 60
ip source-address 10.1.68.78 port 2000
max-redirect 20
system message "SRST Mode: Cisco Unified CME"
keepalive 10
max-conferences 8 gain -6
moh welcome.au
create cnf-files version-stamp Jan 01 2002 00:00:00
```

Step 2  
Use the `show telephony-service ephone-dn` command during fallback to review ephone-dn configurations. Learned ephone-dns are noted by a line stating that they were learned during SRST fallback.

**Note**  
Learned ephone-dns do not appear in the output for the `show running-config` command if the `none` keyword is used in the `srst mode` command.

```
ephone-dn 1 dual-line
number 4008
name 4008
description 4008
preference 0 secondary 9
huntstop
no huntstop channel
call-waiting beep
ephone-dn-template 8
This DN is learned from srst fallback ephones
```
Step 3  Use the show telephony-service ephone command during fallback to review ephone configurations. Learned ephones are noted by a line stating that they were learned during SRST fallback.

Note  Learned ephones do not appear in the output for the show running-config command if the none keyword is used in the srst mode command.

```
ephone 1  
  mac-address 0112.80B3.9C16  
  button 1:1  
  multicast-moh  
  ephone-template 5  
  Always send media packets to this router: No  
  Preferred codec: g711ulaw  
  user-locale JP  
  network-locale US  
  Description: "YOUR Description" : Oct 11 2005 09:58:27  
  This is a srst fallback phone
```

Examples

The following example enables SRST mode on the Cisco Unified CME router. It specifies that learned fallback ephone-dns should be created in dual-line mode and use ephone-dn template 3 for their configuration parameters. Learned ephones will use the parameters in ephone template 5 and a description will be associated with the phones.

```
telephony-service  
  srst mode auto-provision all  
  srst dn line-mode dual  
  srst dn template 3  
  srst ephone description srst fallback auto-provision phone  
  srst ephone template 5
```

The following excerpt from the show running-config command displays the configuration of ephone 1, which was learned during fallback; the description is stamped with the date and time that the show running-config command was used. The configuration of ephone 2, which was prebuilt rather than learned, is shown for comparison.

```
ephone 1  
  description srst fallback auto-provision phone : Jul 07 2005 17:45:08  
  ephone-template 5  
  mac-address 100A.7052.2AAE  
  button 1:1 2:2
```

```
ephone 2  
  mac-address 1002.CD64.A24A  
  type 7960  
  button 1:3
```
The following excerpt from the `show running-config` command displays the configuration of ephone-dn 1 through ephone-dn 3. All three ephones are learned ephone-dns that are configured in dual-line mode and use ephone-dn template 5, as specified in the telephony-service configuration mode commands.

```
ephone-dn  1 dual-line
  number 7001
  description 7001
  name 7001
  ephone-dn-template 5
  This DN is learned from srst fallback ephones

ephone-dn  2 dual-line
  number 4005
  name 4005
  ephone-dn-template 5
  This DN is learned from srst fallback ephones

ephone-dn  3 dual-line
  number 4002
  label 4002
  name 4002
  ephone-dn-template 5
  This DN is learned from srst fallback ephones
```

### Prebuilding Cisco Unified CME Ephone-dn Configurations

This task is optional. It allows you to create a set of ephone-dns that are preconfigured with extension numbers and some features, which will provide service during fallback that is similar to the service that is provided during normal operation. You can prebuild all of your normal extensions, a limited set of your extensions, or none of your extensions. The extensions that are not prebuilt will be populated with extension numbers and features as they are “learned” by the Cisco Unified CME router in SRST mode at the time of fallback.

The prebuilding task establishes ephone-dns to assign to fallback phones as well as to the features with which they should be provisioned.

An ephone-dn is the IP equivalent of a normal phone line in most cases. It represents a potential call connection and is associated with a virtual voice port and virtual dial peer. An ephone-dn has one or more extension or telephone numbers associated with it, which allow call connections to be made. An ephone-dn can be single-line, which allows one call connection to be made at a time, or dual-line, which allows two simultaneous call connections. Dual-line ephone-dns are useful for features such as call transfer or call waiting, in which one call is put on hold to connect to another. Single-line ephone-dns are required for certain features such as intercom, paging, and message-waiting indication (MWI). For more information, see the “Ephone-dns” section in the “Cisco Unified CallManager Express Overview” chapter.

The number and type of features that you choose may vary. This section explains how to set up only a few of the most common features to associate with fallback phones, using the following tasks:

- Configuring Ephone-dns, page 583 (Required)
- Configuring Ephone-dn Templates and Ephone Templates for Fallback Phones, page 586 (Optional)
- Configuring Telephony-Service Parameters, page 588 (Optional)
- Configuring Ephone Hunt Groups, page 590 (Optional)
Configuring Ephone-dns

The objective of this task is to establish a bank of ephone-dn entries that correspond to your Cisco Unified CallManager phone extensions. You can also set up optional call-park slots using this task.

SUMMARY STEPS

1. enable
2. configure terminal
3. ephone-dn dn-tag [dual-line]
4. number number [secondary number] [no-reg [both | primary]]
5. name name
6. park-slot [reserved-for extension-number] [timeout seconds limit count] [notify extension-number [only]] [recall] [transfer extension-number] [alternate extension-number] [retry seconds limit count]

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> ephone-dn dn-tag [dual-line]</td>
<td>Enters ephone-dn configuration mode, creates an ephone-dn, and optionally assigns it dual-line status.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# ephone-dn 20</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring SRST fallback support using Cisco Unified CME

**Command or Action**

| Step 4 | number number [secondary number] [no-reg [both | primary]] |
|---|---|
| **Example:** | Router(config-ephone-dn)# number 2345 |

**Purpose**

Configures a valid extension number for this ephone-dn instance.

- *number*—String of up to 16 characters that represents a telephone or extension number to be associated with this ephone-dn.
- *secondary*—(Optional) Allows you to associate a second telephone number with an ephone-dn.
- *no-reg*—(Optional) Specifies that this number should not register with the H.323 gatekeeper. Unless you specify one of the optional keywords (both or primary) after the no-reg keyword, only the secondary number is not registered.

**Step 5**

<table>
<thead>
<tr>
<th>name name</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
</tr>
</tbody>
</table>

(Optional) Associates a name with this ephone-dn instance. This name is used for caller-ID displays and in the local directory listings.
**Step 6**

**park-slot** [reserved-for extension-number]  
[timeout seconds limit count] [notify extension-number [only]] [recall] [transfer extension-number] [alternate extension-number] [retry seconds limit count]

**Example:**

Router(config-ephone-dn)# park-slot  
reserved-for 2458 timeout 60 limit 3 recall alternate 3754

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>park-slot</td>
<td>(Optional) Creates a floating extension (ephone-dn) at which calls can be temporarily held (parked).</td>
</tr>
<tr>
<td>reserved-for</td>
<td>(Optional) Indicates that this slot is a private slot for the phone with the specified extension number as its primary line. All lines on that phone can use this park slot but no other lines.</td>
</tr>
<tr>
<td>timeout seconds</td>
<td>(Optional) Sets the length of a call-park reminder interval, in seconds. Range is from 0 to 65535. When the interval expires, the call-park reminder sends a 1-second ring and displays a message on the LCD panel of the Cisco Unified IP phone that parked the call and that of any extension that is specified with the notify keyword.</td>
</tr>
<tr>
<td>limit count</td>
<td>(Optional, used with timeout keyword) Sets a limit for the number of timeout intervals for a parked call. Range is 1 to 65535. For example, a limit of 3 sends 2 reminder rings (interval 1, ring 1, interval 2, ring 2, interval 3). A call parked at this slot is disconnected after the limit has been reached unless another action has been specified.</td>
</tr>
<tr>
<td>notify extension-number</td>
<td>(Optional) Sends a reminder ring to the phone with the specified extension in addition to the phone that parked the call. Default is that the reminder ring is sent only to the phone that parked the call.</td>
</tr>
<tr>
<td>only</td>
<td>(Optional) Sends a reminder ring only to the extension specified with the notify keyword and does not send a reminder ring to the phone that parked the call.</td>
</tr>
<tr>
<td>recall</td>
<td>(Optional) Returns the call to the phone that parked it after the timeout intervals expire.</td>
</tr>
<tr>
<td>transfer extension-number</td>
<td>(Optional) Returns the call to the specified extension after the timeout intervals expire.</td>
</tr>
<tr>
<td>alternate extension-number</td>
<td>(Optional) Returns the call to the specified second extension if the recall or transfer target phone is in use on any of its extensions (ringing or in conversation).</td>
</tr>
<tr>
<td>retry seconds</td>
<td>(Optional) Sets the delay before another attempt to recall or transfer a parked call, in seconds. Range is from 0 to 65535. Number of attempts is set by the limit keyword.</td>
</tr>
<tr>
<td>limit count</td>
<td>(Optional, used with retry keyword) Sets a limit for the number of retries. When a limit is set, a call parked at this slot is disconnected after the limit has been reached. Range is from 1 to 65535.</td>
</tr>
</tbody>
</table>
Verifying Ephone-dn Configuration

Step 1  Use the `show telephony-service ephone-dn` command to display ephone-dn configurations.

Examples

The following example sets up five ephone-dns and two call-park slots that will be used for fallback phones.

ephone-dn 1
number 1101
name Register 1

ephone-dn 2
number 1102
name Register 2

ephone-dn 3
number 1103
name Register 3

ephone-dn 4
number 1104
name Register 4

ephone-dn 5
number 1105
name Register 5

ephone-dn 21
number 1121
name Park Slot 1
park-slot timeout 60 limit 3 recall alternate 1100

ephone-dn 22
number 1122
name Park Slot 2
park-slot timeout 60 limit 3 recall alternate 1100

Configuring Ephone-dn Templates and Ephone Templates for Fallback Phones

In this task you build an ephone-dn template and an ephone template that will be applied to extensions and phones when the Cisco Unified CME router is operating in SRST fallback mode. This task is optional, but it provides an easy way to add a set of the same features to a number of fallback extensions and phones.

The features that you list in the templates are applied to the fallback ephone-dns when you use the `srst dn template` and the `srst ephone template` commands, as described in the “Specifying SRST Mode” section on page 578.

Note that these features can also be applied to individual ephone-dns or ephones by using the commands in ephone-dn or ephone configuration mode.
The features that can be implemented using templates are listed in CLI help. Use the following syntax to list the commands that are available:

```
Router(config)# ephone-dn-template
Router(config-ephone-dn-template)# ?
Router(config)# exit
Router(config)# ephone-template
Router(config-ephone-template)# ?
```

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `ephone-dn-template template-tag`
4. `command`
5. `exit`
6. `ephone-template template-tag`
7. `command`
8. `exit`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td>enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> ephone-dn-template</td>
<td>Enters ephone-dn-template configuration mode to create an ephone-dn</td>
</tr>
<tr>
<td>template-tag</td>
<td>template.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# ephone-dn-template</td>
<td>template-tag—Unique identifier for the ephone-dn template that is</td>
</tr>
<tr>
<td>3</td>
<td>being created. Range is from 1 to 20.</td>
</tr>
<tr>
<td><strong>Step 4</strong> command</td>
<td>Applies the specified command to the ephone-dn template that is being</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>created. See CLI help for a list of commands that can be used in this</td>
</tr>
<tr>
<td>Router(config-ephone-dn-template)#</td>
<td>step. Repeat this step to add more commands to the template.</td>
</tr>
<tr>
<td>pickup-group 24</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> exit</td>
<td>Exits ephone-dn-template configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-ephone-dn-template)#</td>
<td>exit</td>
</tr>
</tbody>
</table>
Configuring SRST fallback support using Cisco Unified CME

Verifying Ephone-dn and Ephone Templates for Fallback Phones

Step 1
Use the `show telephony-service ephone-dn-template` and `show telephony-service ephone-template` commands to display the contents of templates for verification of the configured features.

Examples

The following example creates ephone-dn template 3 and ephone template 5 that will be used with the SRST fallback support using Cisco Unified CME feature. Ephone-dn template 3 adds the fallback phones to pickup group 24 and specifies call forwarding for busy and no-answer conditions to extension 1100. Ephone template 5 defines two fastdial numbers that will appear as menu entries displayed from the Directories > Local Services > Personal Speed Dials option on the fallback phones, and also specifies the soft-key layouts for the fallback phones.

```
ephone-dn-template 3
  pickup-group 24
  call-forward busy 1100
  call-forward noan 1100 timeout 45

ephone-template 5
  fastdial 1 1101 name Front Register
  fastdial 2 1100 name Headquarters
  softkeys idle Newcall Cfwdall Pickup
  softkeys seized Endcall Cfwdall Pickup
  softkeys alerting Endcall
  softkeys connected Endcall Hold Park Trnsfer
```

Configuring Telephony-Service Parameters

Some phone features that apply equally to all ephone-dns and ephones are configured in telephony-service mode. An especially useful feature for fallback phones is the use of the `no service directed-pickup` command, which changes the behavior of the Pickup soft key in Cisco Unified CME to match that of the Pickup soft key in Cisco Unified CallManager. For links to other features that are configured in telephony-service mode, see the “Feature Map” section on page xxiii.
### SUMMARY STEPS

1. enable
2. configure terminal
3. telephony-service
4. no service directed-pickup
5. create cnf-files
6. reset all

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> telephony-service</td>
<td>Enters telephony-service configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# telephony-service</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> service directed-pickup</td>
<td>(Optional) Disables directed call pickup and changes the behavior of the PickUp soft key so that a user pressing it invokes local group pickup rather than directed call pickup. This behavior is consistent with that of the PickUp soft key in Cisco Unified CallManager.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(telephony)# no service directed-pickup</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> create cnf-files</td>
<td>Builds XML configuration files for Cisco Unified IP phones.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(telephony)# create cnf-files</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> reset all</td>
<td>Resets all phones.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(telephony)# reset all</td>
<td></td>
</tr>
</tbody>
</table>
Verifying Telephony-Service Parameters

**Step 1**
Use the `show telephony-service all` command to display telephony-service parameters.

Examples

The following example changes the behavior of the Pickup soft key to be like the one in Cisco Unified CallManager.

```
telephony-service
no service directed-pickup
create cnf-files
```

Configuring Ephone Hunt Groups

Ephone hunt groups can be preconfigured for SRST fallback support using Cisco Unified CME if the extensions that are going to be members of the hunt group have already been created using the steps in the “Configuring Ephone-dns” section on page 583.

**Note**
This task shows how to configure one type of hunt group, a peer hunt group, with simple options. For more information about types of hunt groups and their options, see the “Ephone Hunt Groups” section on page 396.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. ephone-hunt hunt-tag {peer | sequential | longest-idle}
4. pilot number [secondary number]
5. list dn-number, dn-number[, dn-number...]
6. hops number
7. timeout seconds[, seconds...]
8. max-timeout seconds
9. final final-number
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
  - Enter your password if prompted. |
| **Example:**  
  Router> enable | |
| **Step 2** configure terminal | Enters global configuration mode. |
| **Example:**  
  Router# configure terminal | |
| **Step 3** ephone-hunt hunt-tag {peer | sequential | longest-idle} | Enters ephone-hunt configuration mode to define an ephone hunt group.  
  - **hunt-tag**—Unique sequence number that identifies this hunt group during all configuration tasks. Range is from 1 to 100.  
  - **peer**—Call-hunt pattern will be peer, meaning that the first ephone-dn to ring is the number to the right of the ephone-dn that was the last to ring when the pilot number was last called. Ringing proceeds in a circular manner, left to right, for the number of hops specified when the ephone hunt group was defined.  
  - **sequential**—Call-hunt pattern will be sequential, meaning that ephone-dns ring in the left-to-right order in which they are listed when the hunt group is defined.  
  - **longest-idle**—Call-hunt pattern will be longest-idle, meaning that calls go to the ephone-dn that has been idle the longest for the number of hops specified when the ephone hunt group was defined. The longest-idle is determined from the last time that a phone registered, reregistered, or went on-hook. |
| **Example:**  
  Router(config)# ephone-hunt 3 peer | |
| **Step 4** pilot number [secondary number] | Defines the pilot number, which is the number that callers dial to reach the hunt group.  
  - **number**—E.164 number with a maximum length of 27 characters. The dialplan pattern can be applied to the pilot number.  
  - **secondary**—(Optional) Defines the number that follows as an additional pilot number for the ephone hunt group. |
| **Example:**  
  Router(config-ephone-hunt)# pilot 1111 | |
### Command or Action

#### Step 5
```
list dn-number, dn-number[, dn-number...]
```

**Example:**
```
Router(config-ephone-hunt)# list 1101, 1102, 1103
```

**Purpose:** Defines the list of numbers to which the ephone hunt group redirects the incoming calls that are made to the pilot number. There must be from 1 to 20 numbers in the list.

- **dn-number**—An ephone-dn primary or secondary number. In Cisco Unified CME 4.0 and later versions, up to three asterisk wildcards (*) can be used in place of standard ephone-dns. The asterisk is a placeholder for any extension that has been allowed to join ephone hunt groups using the `ephone-hunt login` command under the ephone-dn.

#### Step 6
```
hops number
```

**Example:**
```
Router(config-ephone-hunt)# hops 3
```

**Purpose:** (Peer and longest-idle hunt groups only) Sets the number of hops before a call proceeds to the final number.

- **number**—Number of hops. Range is from 2 to 20, but must be less than or equal to the number of extensions that are specified in the list command. Default automatically adjusts to the number of hunt group members.

#### Step 7
```
timeout seconds[, seconds...]
```

**Example:**
```
Router(config-ephone-hunt)# timeout 25
```

**Purpose:** (Optional) Sets the number of seconds after which an unanswered call is redirected to the next number in the hunt-group list. If this command is not used, the default is the time period set by the `timeouts ringing` command, which has a default of 180 seconds if it is not set to another value.

- **seconds**—Number of seconds. Range is from 3 to 60000. In Cisco Unified CME 4.0 and later versions, multiple entries can be made, separated by commas; the number of entries must correspond to the number of ephone-dns in the `list` command. Each number in a multiple entry specifies the time that the corresponding ephone-dn will ring before a call is forwarded to the next number in the list. If a single number is entered, it is used for the no-answer period for each ephone-dn.

**Note** Although the `timeout` command is optional, note that the default of 180 seconds maybe greater than you desire.

#### Step 8
```
final final-number
```

**Example:**
```
Router(config-ephone-hunt)# final 1100
```

**Purpose:** Defines the last number in the ephone hunt group, after which the call is no longer redirected.

- **final-number**—Ephone-dn primary or secondary number, voice-mail pilot number, pilot number of another hunt group, or FXS number.

**Note** Do not use this command if this hunt group is part of a Cisco Unified CME B-ACD application. The final destination for the call is determined by the B-ACD service.
Examples

The following example creates a peer hunt group with the pilot number 1111.

ephone-hunt 3 peer
pilot 1111
list 1101, 1102, 1103
hops 3
timeout 25
final 1100

Examples

The following example shows a Cisco Unified CME system at 10.1.68.78 that is being used to provide SRST fallback services for 30 ephones.

telephony-service
srst mode auto-provision all
srst ephone template 5
srst ephone description srst fallback auto-provision phone
srst dn template 8
srst dn line-mode dual
max-ephones 30
max-dn 60
ip source-address 10.1.68.78 port 2000
max-redirect 20
system message "SRST Mode: Cisco Unified CME"
keepalive 10
max-conferences 8 gain -6
moh welcome.au
create cnf-files version-stamp Jan 01 2002 00:00:00
!
ephone-dn 1 dual-line
number 7001
label 7001
description 7001
name 7001
ephone-dn-template 5
This DN is learned from srst fallback ephones
!
!
ephone-dn 2 dual-line
number 4005
description 4005
name 4005
ephone-dn-template 5
This DN is learned from srst fallback ephones
!
!
ephone-dn 3 dual-line
number 4002
label 4002
description 4002
name 4002
ephone-dn-template 5
This DN is learned from srst fallback ephones
!
ephone 1
description srst fallback auto-provision phone
ephone-template 5
mac-address 100A.7052.2AAE
button 1:1 2:2
!
ephone 2
description srst fallback auto-provision phone
ephone-template 5
mac-address 1002.CD64.A24A
type 7960
button 1:3

**Feature History for SRST Fallback Support Using Cisco Unified CME**

<table>
<thead>
<tr>
<th>Cisco Unified CME Version</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.0</td>
<td>SRST fallback support using Cisco Unified CME was introduced.</td>
</tr>
</tbody>
</table>

**Related Features**

**Cisco Unified CallManager**
For more information about Cisco Unified CallManager, see the [Cisco Unified CallManager technical documentation website](#).

**Cisco Unified IP Phones**
For links to more information about Cisco Unified IP phones that are used with Cisco Unified CME, see the [Cisco Unified CallManager Express Documentation Roadmap](#).

**Cisco Unified CME Features**
For links to information about specific features, see the [Cisco Unified CME Feature Map](#).
Loopback Call Routing

Loopback call routing in a Cisco Unified CallManager Express (Cisco Unified CME) system is provided through a mechanism called loopback-dn, which provides a software-based limited emulation of back-to-back physical voice ports connected together to provide a loopback call-routing path for voice calls. This chapter includes the following sections:

- Loopback Call Routing Overview, page 595
- Configuring Loopback Call Routing, page 596
- Verifying Loopback Call Routing, page 600
- Examples, page 600
- Feature History for Loopback Call Routing, page 600

Note

Loopback Call Routing Overview

Note
For a summary of the functionality introduced in different releases, see the “Feature History for Loopback Call Routing” section on page 600.

The primary use of loopback call routing and loopback-dn is to restrict the passage of call-transfer and call-forwarding supplementary service requests through the loopback. Instead of passing these requests through, the loopback-dn mechanism attempts to service the requests locally. This allows loopback-dn configurations to be used in call paths where one of the external devices does not support call transfer or call forwarding (Cisco-proprietary or H.450-based). Control messages that request call transfer or call forwarding are intercepted at the loopback virtual port and serviced on the local voice gateway. If needed, this mechanism creates VoIP-to-VoIP call-routing paths.

Loopback call routing may be used for routing H.323 calls to Cisco Unity Express. For more information, see Integrating Cisco CallManager Express and Cisco Unity Express. For information about Cisco Unity Express configuration, see the Cisco Unity Express documentation.
A preferred alternative to loopback call routing was introduced in Cisco CME 3.1. This alternative blocks H.450-based supplementary service requests by using the following CLI commands: `no supplementary-service h450.2`, `no supplementary-service h450.3`, and `supplementary-service h450.12`. For more information, see the “Transfer and Forwarding Support” section on page 223.

Use of loopback-dn configurations within a VoIP network should be restricted to resolving critical network interoperability service problems that cannot otherwise be solved. Loopback-dn configurations are intended to be used in VoIP network interworking situations in which the only alternative would be to make use of back-to-back-connected physical voice ports. Loopback-dn configurations emulate the effect of a back-to-back physical voice-port arrangement without the expense of the physical voice-port hardware. Because digital signal processors (DSPs) are not involved in loopback-dn arrangements, the configuration does not support interworking or transcoding between calls that use different voice codecs. In many cases, use of back-to-back physical voice ports that do involve DSPs to resolve VoIP network interworking issues is preferred, because it introduces fewer restrictions in terms of supported codecs and call flows. Also, loopback-dns do not support T.38 fax relay.

### Configuring Loopback Call Routing

Loopback call routing requires two extensions (ephone-dns) to be separately configured, each as half of a loopback-dn pair, as described in this task. In addition to defining the loopback-dn pair, you must specify preference, huntstop, class of restriction (COR), and translation rules. Ephone-dns that are defined using the `loopback-dn` command are never associated with a physical phone; they are used only for loopback call routing.

#### SUMMARY STEPS

1. `ephone-dn dn-tag`
2. `number number [secondary number] [no-reg [both | primary]]`
3. `caller-id {local | passthrough}`
4. `no huntstop`
5. `preference preference-order [secondary secondary-order]`
6. `cor {incoming | outgoing} cor-list-name`
7. `translate {called | calling} translation-rule-tag`
8. `loopback-dn dn-tag [forward number-of-digits | strip number-of-digits] [prefix prefix-digit-string] [suffix suffix-digit-string] [retry seconds] [auto-con] [codec {g711alaw | g711ulaw}]`
9. `exit`
10. Repeat Steps 1 through 8 using a second ephone-dn to complete the loopback-dn pair.
## DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** ephone-dn `dn-tag` | Enters ephone-dn configuration mode, creates an ephone-dn, and optionally assigns it dual-line status.  
  - `dn-tag`—Unique sequence number that identifies this ephone-dn during configuration tasks. Range is platform- and version-dependent. Refer to command-line interface (CLI) help.  
  **Note** Ephone-dns used for loopback cannot be dual-line ephone-dns. |
| **Example:**  
Router(config)# ephone-dn 15 |

| **Step 2** number `number` [secondary `number`] [no-reg [both | primary]] | Associates a number with this extension (ephone-dn).  
  - `number`—String of up to 16 digits that represents a telephone or extension number to be associated with this ephone-dn.  
  - secondary—(Optional) Allows you to associate a second telephone number with an ephone-dn.  
  - no-reg—(Optional) Specifies that this number should not register with the H.323 gatekeeper. The `no-reg` keyword by itself indicates that only the secondary number should not register. The `no-reg both` keywords indicate that both numbers should not register, and the `no-reg primary` keywords indicate that only the primary number should not register. |
| **Example:**  
Router(config-ephone-dn)# number 2001 |

| **Step 3** caller-id (local | passthrough) | Specifies caller-ID treatment for outbound calls originated from the ephone-dn. The default if this command is not used is as follows. For transferred calls, caller ID is provided by the number and name fields from the outbound side of the loopback-dn. For forwarded calls, caller ID is provided by the original caller ID of the incoming call. Settings for the `caller-id block` command and translation rules on the outbound side are executed.  
  - local—Passes the local caller ID on redirected calls. This is the preferred usage.  
  - passthrough—Passes the original caller ID on redirected calls. |
| **Example:**  
Router(config-ephone-dn)# caller-id local |

| **Step 4** no huntstop | Disables huntstop and allows call hunting behavior for an extension (ephone-dn). |
| **Example:**  
Router(config-ephone-dn)# no huntstop |
### Command or Action

<table>
<thead>
<tr>
<th>Step 5</th>
<th>preference preference-order [secondary secondary-order]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>Router(config-ephone-dn)# preference 1</td>
</tr>
</tbody>
</table>

Sets dial-peer preference for an extension (ephone-dn).

- **preference-order**—Preference order for the primary number associated with an extension (ephone-dn). Range is from 0 to 10, where 0 is the highest preference and 10 is the lowest preference. Default is 0.
- **secondary secondary-order**—(Optional) Preference order for the secondary number associated with the ephone-dn. Range is from 0 to 10, where 0 is the highest preference and 10 is the lowest preference. Default is 9.

| Step 6 | cor {incoming | outgoing} cor-list-name |
|--------|------------------------------------|
| Example: | Router(config-ephone-dn)# cor incoming corlist1 |

Applies a class of restriction (COR) to the dial peers associated with an extension. COR is used to specify which incoming dial peer can use which outgoing dial peer to make a call. Each dial peer can be provisioned with an incoming and an outgoing COR list.

For information about COR, see the “Configuring Dial Peer Matching Features” section in “Dial Peer Configuration on Voice Gateway Routers” at the Cisco IOS Voice Configuration Library.

| Step 7 | translate {called | calling} translation-rule-tag |
|--------|---------------------------------------------|
| Example: | Router(config-ephone-dn)# translate called 1 |

Selects an existing translation rule and applies it to a calling number or a number that has been called. This command enables the manipulation of numbers as part of a dial plan to manage overlapping or nonconsecutive numbering schemes.

- **called**—Translates the called number.
- **calling**—Translates the calling number.
- **translation-rule-tag**—Unique sequence number of the previously defined translation rule. Range is from 1 to 2147483647.

**Note** This command requires that you have previously defined appropriate translation rules using the **voice translation-rule** and **rule** commands.
### Command or Action

**Step 8**

```
loopback-dn dn-tag [forward number-of-digits | strip number-of-digits] [prefix prefix-digit-string] [suffix suffix-digit-string] [retry seconds] [auto-con] [codec {g711alaw | g711ulaw}]
```

### Purpose

 Enables H.323 VoIP call transfer and call forwarding by using hairpin call routing for VoIP endpoints that do not support the Cisco-proprietary call-transfer and call-forwarding mechanism.

- **dn-tag**—Unique sequence number that identifies the ephone-dn that is being paired for loopback with the ephone-dn that is currently being configured. The paired ephone-dn must be one that is already defined in the system.

- **forward number-of-digits**—(Optional) Number of digits in the original called number to forward to the other ephone-dn in the loopback-dn pair. Range is from 1 to 32. Default is to forward all digits.

- **strip number-of-digits**—(Optional) Number of leading digits to be stripped from the original called number before forwarding to the other ephone-dn in the loopback-dn pair. Range is from 1 to 32. Default is to not strip any digits.

- **prefix prefix-digit-string**—(Optional) Defines a string of digits to add in front of the forwarded called number. Maximum number of digits in the string is 32. Default is that no prefix is defined.

- **suffix suffix-digit-string**—(Optional) Defines a string of digits to add to the end of the forwarded called number. Maximum number of digits in the string is 32. Default is that no suffix is defined. If you add a suffix that starts with the pound character (#), the string must be enclosed in quotation marks.

- **retry seconds**—(Optional) Number of seconds to wait before retrying the loopback target when it is busy or unavailable. Range is from 0 to 32767. Default is that retry is disabled and appropriate call-progress tones are passed to the call originator.

- **auto-con**—(Optional) Immediately connects the call and provides in-band alerting while waiting for the far-end destination to answer. Default is that automatic connection is disabled.

- **codec**—(Optional) Explicitly forces the G.711 A-law or G.711 mu-law voice coding type to be used for calls that pass through the loopback-dn. This overrides the G.711 coding type that is negotiated for the call and provides conversion from mu-law to A-law if needed. Default is that Real-Time Transport Protocol (RTP) voice packets are passed through the loopback-dn without considering the G.711 coding type negotiated for the calls.

  - **g711alaw**—G.711 A-law, 64000 bits per second, for T1.
  - **g711ulaw**—G.711 mu-law, 64000 bits per second, for E1.

### Example:

Router(config-ephone-dn)# loopback-dn 24 forward 15 prefix 415353....
Verifying Loopback Call Routing

Step 1
Use the `show running-config` or `show telephony-service ephone-dn` command to display ephone-dn configurations.

Examples

The following example uses ephone-dns 15 and 16 as a loopback-dn pair. Calls are routed through this loopback ephone-dn pair in the following way:

- An incoming call to 4085552xxx enters the loopback pair through ephone-dn 16 and exits the loopback via ephone-dn 15 as an outgoing call to 2xxx (based on the forward 4 digits setting).
- An incoming call to 6xxx enters the loopback pair through ephone-dn 15 and exits the loopback via ephone-dn 16 as an outgoing call to 4157676xxx (based on the prefix 415767 setting).

```
ephone-dn 15
  number 6...
  loopback-dn 16 forward 4 prefix 415767
caller-id local
  no huntstop
!
!
ephone-dn 16
  number 4085552...
  loopback-dn 15 forward 4
caller-id local
  no huntstop
```

Feature History for Loopback Call Routing

<table>
<thead>
<tr>
<th>Cisco Unified CME Version</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.0</td>
<td>Loopback call routing was introduced.</td>
</tr>
</tbody>
</table>
Index

A

abbreviated dialing 528
account code entry 492, 493
Acct soft key 552
after-hour exempt command 448
after-hours block pattern command 446
after-hours date command 447
after-hours day command 447
after-hours toll bar 444
agent availability, ephone hunt groups 401
agent status control, ephone hunt groups 403
alerting (call stage) 551
all-call call forwarding 372
allow-connections command 248
alternative user and network locales 97
analog phones 138
API, XML 360
archives, downloading for Cisco Unified CME 46
associate application command 212
associate ccm command 210
associate profile command 210
ATA (Cisco Analog Telephone Adapters) 138
audio fallback, for video calls 286
audio file for MOH 48
audio paging 342
authentication, See phone authentication
authentication for HTTP server 125
authentication string, entering on phone 191
auth-mode command 189
auth-string command 189
auto-answer, headset 508
auto-cut-through command 339
auto-line command 495
auto logout command 404
automatic agent status not-ready, ephone hunt groups 404
automatic line selection 493
automatic registration blocking 65
auto-reg-ephone command 65

B

backup router 351
bandwidth, for video 295
beep, call-waiting 392
bit-rate, setting maximum value 294
blocking
automatic registration 65
caller ID 475
call park 458
calls 444
call transfer 467
class of restriction 497
features 329
local directory 315
bulk-loading speed-dial numbers 532
bulk-speed-dial list command 534
bulk-speed-dial-prefix command 534
busy call forwarding 372
busy subscriber callback 496
busy timeout 355
button command 75
feature ring 75
normal ring 75
overlaid ephone-dns 434
silent ring 75
CA (certification authority) 151
callback busy subscriber 496
Callback soft key 552
call blocking
  based on date and time 444
  class of restriction (COR) 497
  override 445
call-coverage features 369
called-name display 537
caller-id block command 477
caller ID blocking 475, 476
caller-id command 597
call-forward all command 375
call-forward busy command 375
call forwarding 372
  blocking local extension forwards 376
Cisco proprietary method 224
examples 377
H.450.3 standard 224, 225
H.450 standards 372
selective 373
SIP networks 276
Tcl script 224
transcoding between G.726 and G.711 199
verifying and troubleshooting 256

call-forward max-length command 376
call-forward night-service command 376
call-forward noan command 376
call-forward pattern command 278, 373, 374
call-forward pattern command (SIP trunks) 278
call hold 450
call hunt 379
  examples 383
calling-number local command 278
call-manipulation features 443
call park 454
  alternate target 456
  blocking 458
call-park slots 454
dedicated slots 456
directed 455
examples 462
monitoring call-park slots 455
redirect 458
reminder ring 456
timeout interval 456
call-park system redirect command 291, 461
call pickup
  examples 390
    group numbers 386
call routing, loopback 595
call setup, video 286
call start slow command 290
call transfer 465
  blocking 467
Cisco proprietary method 224
consult transfer for direct station select 466
direct station select 466
examples 473
H.450.2 standard 224, 225
H.450 standards 465
SIP networks 276
speed-dial numbers 467
Tcl script 224
transcoding between G.726 and G.711 199
transfer-system setting 466
verifying and troubleshooting 256
call type 286
call waiting 391
  beep 392
  examples 395
  overlaid ephone-dns 430
restrictions 393
  ring 392
call-waiting beep command 392, 394
call-waiting ring command 392, 394
<p>| Index |
|-----------------|-----------------|
| <strong>CAPF (certificate authority proxy function)</strong> | 153 |
| capf-auth-str command | 176 |
| capf-server command | 188 |
| cautions | usage in text | xxxi |
| cert-enroll-trustpoint command | 188 |
| certificate | 151 |
| certificate authority proxy function, See CAPF |  |
| certificate revocation list, See CRL |  |
| certificates | 150 |
| certificate trust list, See CTL |  |
| certification authority, See CA |  |
| cert-oper (CAPF-server) command | 190 |
| cert-oper (ephone) command | 177 |
| CFwdALL soft key | 552 |
| channel huntstop | 381 |
| CIF (common intermediate format) | 288 |
| Cisco BTS Softswitch (Cisco BTS) | 225, 226, 227, 229, 231 |
| Cisco IOS software support | 2 |
| Cisco IP Communicator | 140 |
| Cisco PSTN Gateway (Cisco PGW) | 225, 226, 229, 231 |
| Cisco Unified CallManager |  |
| fallback support using Cisco Unified CME | 573 |
| interworking with Cisco Unified CME | 249, 253 |
| network scenario | 236, 237 |
| no support for H.450 standards | 226 |
| video support | 287 |
| Cisco Unified CallManager Express (Cisco Unified CME) |  |
| basic concepts | 24 |
| description | 21 |
| downloading files | 46 |
| enabling video | 291 |
| feature history | 1 |
| license requirements | 40 |
| prerequisites | 39 |
| restrictions | 41 |
| specifications | 2 |
| video support | 287 |
| Cisco Unified Video Advantage | 288 |
| Cisco Unity Express |  |
| integration with Cisco Unified CME | 300 |
| transcoding between G.726 and G.711 | 199 |
| Cisco Unity integration | 301 |
| Cisco VG 224 | 138 |
| class of restriction (COR) | 497 |
| clear telephony-service xml-event-log command | 365 |
| clid strip command | 478 |
| clid strip name command | 478 |
| client identifier command | 55 |
| clock summer-time command | 58 |
| clock timezone command | 58 |
| cnf-file command | 96 |
| cnf-file location command | 96 |
| cnf-file perphone command | 174 |
| codec (dspfarm-profile) command | 211 |
| codec, for remote phones | 144 |
| codec command | 147 |
| command syntax conventions | xxx |
| common intermediate format, see CIF | 288 |
| conferencing | 480 |
| end-of-conference options | 481 |
| examples | 485 |
| gain control | 481 |
| initiator dropoff control | 481 |
| transcoding between G.729 and G.711 for ad hoc calls | 199 |
| configuration files | 91 |
| externally stored | 93 |
| GUI | 129 |
| per phone | 93 |
| per phone type | 93 |
| Confrn soft key | 552 |
| connected (call stage) | 551 |
| connection plar-opx command | 267 |
| conventions, document | xxix |
| COR (class of restriction) | 498 |
| corlist command | 499 |
| CPU consumption, for video calls | 289 |</p>
<table>
<thead>
<tr>
<th>Index</th>
</tr>
</thead>
<tbody>
<tr>
<td>create cnf-files command 66, 291</td>
</tr>
<tr>
<td>credentials command 185</td>
</tr>
<tr>
<td>CRL (certificate revocation list) 152</td>
</tr>
<tr>
<td>crypto pki authenticate command 167, 169</td>
</tr>
<tr>
<td>crypto pki enroll command 167</td>
</tr>
<tr>
<td>crypto pki server command 159, 161, 164</td>
</tr>
<tr>
<td>crypto pki trustpoint command 160, 163, 166, 169</td>
</tr>
<tr>
<td>CTL (certificate trust list) 152</td>
</tr>
<tr>
<td>ctl-client command 180, 183</td>
</tr>
<tr>
<td>ctl-service admin command 186</td>
</tr>
<tr>
<td>customer administrator GUI access setup 129</td>
</tr>
<tr>
<td>using the CLI 133</td>
</tr>
<tr>
<td>using the GUI 132</td>
</tr>
</tbody>
</table>

_**D**_

| database level command 159 |
| database url command 160 |
| date-format command 66 |
| debug cch323 video command 296 |
| debug dspfarm command 220 |
| debug ephone detail command 296 |
| debug ephone message command 296 |
| debug ephone mtp command 220 |
| debug ephone register command 296 |
| debug ephone video command 296 |
| debug h225asn1 command 296 |
| debug h245 asn1 command 296 |
| debug sccp command 219 |
| debug voip ccapi inout command 296 |
| dedicated call-park slots 456 |
| default-router command 54, 55 |
| description (ephone-hunt) command 409 |
| description command 549 |
| device-security-mode command 174, 176 |
| DHCP (Dynamic Host Configuration Protocol) service 52 |
| changing TFTP address 57 |
| option 150 and configuration files 91 |
| dialing on-hook 522 |
| dial-peer hunt command 429 |
| dial-peer hunt for ephone-dn dial peers |
| dial-peer preference 380 |
| dial peers ephone-dns and 26 |
| for call transfer and forwarding 256 |
| dialplan-pattern command 116 |
| dial-plan support 113 |
| dial tone, secondary 356 |
| DID (Direct Inward Dialing) 33 |
| digital certificate 151 |
| digital certificates 150 |
| digital signature 151 |
| directed call park 455 |
| directed call pickup, See call pickup directories 315 |
| directory command 316 |
| directory entry command 316 |
| direct station select call transfer 466 |
| display called-name 537 |
| phone header bar 547 |
| soft-key 551 |
| system message 557 |
| display-logout command 409 |
| distinctive ringing 502 |
| DND soft key 403, 552 |
| dn-webedit command 128 |
| document conventions xxix |
| document organization xxviii |
| documents, related 36 |
| Do Not Disturb (DND) 504 |
| dspfarm-assist keyword, for remote phones 144 |
| dspfarm profile command 211 |
| DSP farms, usage considerations 200 |
| dspfarm transcoder maximum sessions command 207, 213 |
| DSPs (digital signal processors) 201 |
| dsp services dspfarm command 206, 208 |
DTMF integration patterns for voice mail 301
DTMF relay
   for H.323 networks 59
   for SIP networks 276
dtmf-relay command (H.323 networks) 60
dtmf-relay command (SIP trunks) 279
dual-line ephone-dn 27
dual-number ephone-dns 29
dynamic membership, ephone hunt groups 403
ephone firmware 288
ephone-hunt command 406
ephone hunt groups 396
agent availability options 401
agent status control 403
automatic agent status not-ready 404
dynamic membership 403
examples 413
final number 397
hops 397
longest-idle groups 400
peer groups 399
restrictions 405
sequential groups 398
ephone-hunt login command 411
ephones
   definition 24
   enabling video 292
   overview 25
   resetting 293
   setting video bandwidth 295
   extending overlaid ephone-dn calls 432
FACs (feature access codes) 325
fastdial command 527
fax support 138
Feature access codes (FACs) 325
feature blocking 329
feature control 329
feature history 1
Feature Navigator 2
feature ring (button command) 75
features
   administrative and system 313
<table>
<thead>
<tr>
<th>call-coverage</th>
<th>369</th>
</tr>
</thead>
<tbody>
<tr>
<td>call-handling</td>
<td>443</td>
</tr>
<tr>
<td>phone</td>
<td>489</td>
</tr>
<tr>
<td>video</td>
<td>285</td>
</tr>
<tr>
<td>features blocked command</td>
<td>330</td>
</tr>
<tr>
<td>FECC (far-end camera control)</td>
<td>288</td>
</tr>
<tr>
<td>files, configuration</td>
<td>91</td>
</tr>
<tr>
<td>files, downloading for Cisco Unified CME</td>
<td>46</td>
</tr>
<tr>
<td>final command</td>
<td>407</td>
</tr>
<tr>
<td>firmware, for video</td>
<td>288</td>
</tr>
<tr>
<td>Flash soft key</td>
<td>552, 561</td>
</tr>
<tr>
<td>flow-around mode, video stream</td>
<td>287</td>
</tr>
<tr>
<td>flow control messages</td>
<td>286</td>
</tr>
<tr>
<td>flow-through mode, video stream</td>
<td>287</td>
</tr>
<tr>
<td>foreign exchange office (FXO) trunk lines</td>
<td>264</td>
</tr>
<tr>
<td>forwarding, See call forwarding</td>
<td></td>
</tr>
<tr>
<td>forward local-calls command</td>
<td>376</td>
</tr>
<tr>
<td>from-ring command</td>
<td>400, 409</td>
</tr>
<tr>
<td>function button customized displays</td>
<td>569</td>
</tr>
<tr>
<td>fwd-final command</td>
<td>408</td>
</tr>
<tr>
<td>FXO hookflash</td>
<td>561</td>
</tr>
<tr>
<td>fxo hook-flash command</td>
<td>562</td>
</tr>
<tr>
<td>FXS ports</td>
<td>138</td>
</tr>
<tr>
<td>restrictions</td>
<td>125</td>
</tr>
<tr>
<td>setting up</td>
<td>125</td>
</tr>
<tr>
<td>system administrator setup</td>
<td>126</td>
</tr>
</tbody>
</table>

**H**

H.225 debug messages | 296 |
H.245 debug messages | 296 |
H.261 video codec   | 288 |
H.263 video codec   | 288 |
H.323-to-H.323 connections, enabling | 248 |
H.323 video endpoints | 285 |
H.450.12 supplementary services | 225 |
  | description | 228 |
  | enabling    | 245 |
H.450.2 supplementary services | 225 |
  | description | 225 |
  | enabling    | 240 |
| handling non-H.450.2 calls | 228 |
| network requirements | 227 |
H.450.3 supplementary services | 225 |
  | description | 225 |
  | enabling    | 240 |
| handling non-H.450.3 calls | 228 |
| network requirements | 227 |
H.450 standards
  | call forwarding | 372 |
  | call transfer   | 465 |
H.450 tandem gateways | 225 |
  | description     | 231 |
  | enabling        | 248 |
| licensing        | 231 |
| restrictions      | 233 |
h225 h245-address on-connect (h323 voice-service) command | 251 |
h225 h245-address on-connect (voice-class) command | 252 |
hairpin call routing | 225 |
  | description     | 229 |
enabling H.323-to-H.323 connections 248
network requirements 230
restrictions 231
Tcl script in Cisco CME 3.0 224
header bar display 547
headset auto-answer 508
headset auto-answer command 511
history, feature 1
HLog soft key 403, 552
hold 450
hold-alert command 452
Hold soft key 552
hookflash, FXO 561
hookflash functionality 561
hops command 397, 407
host command 55
HTTP path, setting 125
HTTP server, enabling 125
hunt, See call hunt
hunt-group logout command 404, 411
hunt groups, See ephone hunt groups
huntstop 380
huntstop (ephone-dn) command 382
huntstop, channel 381
huntstop channel command 382
huntstop channel command, overlaid ephone-dns 433
huntstop command 380, 382
huntstop command, overlaid ephone-dns 429, 433

I

idle (call stage) 552
incoming alerting command (redundant router) 354
input gain command 338
intercom 513
intercom command 516
interdigit timeout 355
interface command 56
international languages and tones 62
alternative locales 97
user-defined locales 105
interoperability with systems other than Cisco Unified CME 224
intersite calling plan 32
ip dhcp pool command 54, 55
ip helper-address command 56
ip http authentication command 126
ip http path flash command 126, 526
ip http server command 126, 526
ip source-address (credentials) command 186
ip source-address command 65, 214
ip source-address command (redundant router) 353
issuer-name command 160
ixi application cme command 362
ixi transport http command 361

K

keepalive command 66
keepalive retries command 210
keep-conference command 481
keygen-retry command 190
keygen-timeout command 190
keyswitch model 33

L

label command 546
labels, ephone-dn 545
label support 545
languages and tones 62
license prerequisites 40
lifetime certificate command 160, 164
line selection, automatic 493
line selection for MWI 519
list command 407
live-feed music on hold 337
load-cfg-file command 175
load command 65
local directory 315
locales, user and network
  alternative 97
  user-defined 105
locally significant certificate, See LSC
local speed dial 525
login (telephony-service) command 447
Login soft key 552
log table max-size command 365
log table retain-timer command 365
longest-idle ephone hunt groups 400
loopback call routing 595
loopback-dn command 599
LSC (locally significant certificate) 153

M
mac-address command 73
mailbox-selection (dial-peer) command 306
mailbox-selection (ephone-dn) command 307
mailbox selection policy 304
manufacture-installed certificate, See MIC
max-conferences command 483
max-dn command 64
max-ephones command 64
maximum bit-rate command 294
maximum sessions command 211
max-redirect command 397, 410
max-timeout command 408
media messages 286
media packet destination for remote phones 144
media path setup 286
media termination point, See MTP
memory prerequisites 40
messages
  debug 296
  flow control 286
  media 286
MIBs 38
MIC (manufacture-installed certificate) 153
  configuring 168
  mode ra command 164
moh (ephone-dn) command 340
MOH (music on hold)
  audio file to download 48
  from a live feed 337
  from an audio file 334
  multicast 336, 340
  transcoding between G.726 and G.711 200
moh (telephony-service) command 335
monitoring call-park slots 455
monitor-line button 524
monitor mode for line button 75
MTP (media termination point)
  remote phones 144
  transcoding for video
  mtp command 146
  multicast moh command 336
  mwi-line command 520
MWI line selection 519
MWI prefix specification for SIP 308
mwi qsig command 273

N
name command 72
network command 54
network-locale (ephone-template) command 101, 108
network-locale command 66, 100, 108
network locales 62
  alternative 97
  user-defined 105
network prerequisites 40
NewCall soft key 552
night service 420
  examples 427
  notification 420
parameters 420
night-service bell (ephone) command 425
night-service bell (ephone-dn) command 424
night-service call forwarding 372
night-service code command 424
night-service date command 423
night-service day command 423
night-service everyday command 423
night-service weekday command 424
night-service weekend command 424
no-answer call forwarding 372
no-reg (ephone-hunt) command 408
normal ring (button command) 75
notes, usage in text xxxi
notification, night-service 420
notification, on-hold 451
notify telephone-event command 280
not-ready, automatic, ephone hunt groups 404
NTP (Network Time Protocol) 57
ntp server command 58
number command 72
number plan 32

O
one-quarter common intermediate format, see QCIF 288
on-hold notification 450, 451
on-hook dialing 522
open logical channel (OLC) 287
operation command 339
option 150 (DHCP)
    and configuration files 91
    changing TFTP address 57
option 150 ip command 54, 55
organization, document xxviii
overlaid ephone-dns 30, 429
call waiting 430
definition 30
examples 435
huntstop 430
preference 429
restrictions 432
rollover to another button 432
override for after-hours toll bar 444

P
packet voice/data modules (PVDM) 201
paging 342
paging command 346
paging-dn command 347
paging group command 347
parking calls 454
park-slot command 460
Park soft key 552
pattern direct command 303
pattern ext-to-ext busy command 303
pattern ext-to-ext no-answer command 303
pattern trunk-to-ext busy command 303
pattern trunk-to-ext no-answer command 303
PBX interworking, QSIG services 270
PBX model 33
peer ephone hunt groups 399
per-phone configuration files 93
personal speed dial 527
phone authentication 149
    authentication string entering on phone 191
    CA configuration 158
    CAPF server configuration 187
certificates 150
Cisco Unified CME server function configuration 165
classification tasks 156
CTL client and CTL provider configuration 179
CTL provider configuration 185
task examples 192
glossary 196
MIC importing 168
PKI 150
RA configuration 162
    telephony-service security configuration 173
    telephony-service security parameters 173
phone display, See display
phone features 489
phone header bar display 547
phone-key-size command 189
phone number plan 32
phones
    See ephone-dns and ephones
phones, analog 138
phones, teleworker remote 143
phone support 137
phone user GUI access setup 134
    using CLI 135
    using GUI 134
pickup, See call pickup
pickup-group command 388
PickUp soft key 552
pilot command 406
PIN (personal identification number) 445
pin command 448
PKI (Public Key Infrastructure) 150
platform support 2
port (CAPF-server) command 188
preference (ephone-dn) command 380, 382
preference (ephone-hunt) command 408
preference, dial-peer 380
preference command, overlaid ephone-dns 429, 433
prerequisites
    installation 39
    licenses 40
    memory 40
    network 40
present-call command 409
private lines to Public Switched Telephone Network (PSTN) 264
profiles, voice translation 117

Q
QCIF (one-quarter common intermediate format) 288
QSIG supplementary services 270

R
RA (registration authority) 152
ready/not-ready status, ephone hunt groups 403
Real-Time Transport Protocol, See RTP
rebooting phones 76
Redial soft key 552
redundant router 351
regenerate command 181, 184
register support, SIP 277
registrar command 280
registration, blocking automatic 65
registration, video-enabled endpoints 288, 293
registration authority, See RA
related documents 36
relay, DTMF 59
reminder, call-park 456
reminder, on-hold 451
remote phones 143
request outstanding command 361
request timeout command 362
reset all command 293
reset command 292
reset ephone 293
resetting phones
    description 76
    reset (ephone) command 77
resolution, for video 288
response size command 361
response timeout command 363
restarting phones
    description 76
    restart (ephone) command 79
restrictions
alternative user and network locales 99
analog FXS ports 139
call blocking 445
called-name display 539
caller ID blocking 476
call waiting 393
configuration files 94
direct FXO trunk lines 265
ephone hunt groups 405
general 41
GUI 125
H.323 to SIP hairpin 248
H.450 tandem gateways 233
hairpin call routing 231
mailbox selection policy 305
music on hold (MOH) 334
music on hold (MOH) from live feed 337
on-hook abbreviated dialing 529
paging 343
SRST fallback support 577
Teleworker remote phones 145
transcoding 201
user and network locales 62
user-defined user and network locales 106
video 288
retry register command 280
revocation-check command 163, 166, 169
RFCs 38
ring, call-waiting 392
ring command 503
ringing, distinctive 502
ringing timeout 355
ring number command (redundant router) 354
rollover button for overlaid ephone-dns 432
routing, loopback 595
RSA key pair 151
rsakeypair command 164, 167
RTP (Real-Time Transport Protocol) 287
rule command 119
rules, voice translation 117
SAST (system administrator security token) 180, 183
sast1 trustpoint command 180, 183
sast2 trustpoint command 180, 183
SCCP (Skinny Client Control Protocol)
  analog phones 138
  security 149
  video support 285
  sccp ccm group command 209
SCCP video endpoints 285
sdspfarm tag command 215
dsdpfarm transcode sessions command 214
secondary dial tone 356
secondary-dialtone command 357
secondary numbers 29
secondary router 351
secondary start command 409
secure-signaling trustpoint command 174
security, See phone authentication
seized (call stage) 552
selective call forwarding 373
sequential ephone hunt groups 398
serial-number command 164
server (CTL-client) command 181
server cme command 181, 184
server-security-mode command 181
service dhcp command 56
service directed-pickup command 389
service local-directory command 316
service phone command 62, 66
service phone pcPort command 565
service phone videoCapability command 291
Session Initiation Protocol, See SIP
shared ephone-dns 29
shared lines 32
Index

show call active video command 296
show call prompt-mem-usage command 261
show capf-server auth-string command 178
show crypto pki certificates command 165, 168
show crypto pki server command 165
show ctl-client command 184
show dspfarm sessions active command 219
show dspfarm sessions command 218
show dspfarm sessions summary command 218
show ephone command 84
show ephone-dn callback command 497
show ephone-dn command 85
show ephone-dn park command 464
show ephone offhook command 296
show ephone phone-load command 288
show ephone registered command 287, 292, 296
show fb-its-log command 365
show rtp connections command 296
show running-config command 83, 295
show sccp command 217
show sccp connections details command 219
show sdspfarm command 218
show sdspfarm connections command 204
show sdspfarm sessions command 204
show sdspfarm units command 204
show sip-ua register status command 282
show sip-ua statistics command 282
show sip-ua status command 282
show sip-ua timers command 282
show telephony-service bulk-speed-dial command 536
show telephony-service security-info command 178
show telephony-service tftp-bindings command 84
show voice dsp command 204
show voip rtp connections command 260, 287
signal immediate command 339
signature 151
single in-line memory module (SIMM) sockets 201
single-line ephone-dn 26
SIP (Session Initiation Protocol)
call forwarding 276
call transfer 276
DTMF relay 276
endpoints 289
register support 277
trunks 275
SIP phones 142
Skinny Client Control Protocol, See SCCP 285
slots, call-park 454
slow start, for video 290
soft key
DND 403
feature control 329
Flash 561
HLog 403
soft-key display 551
softkeys commands 554
software, downloading for Cisco Unified CME 46
source-addr command 188
specifications, Cisco Unified CME 2
speed dial 523
bulk loading 532
buttons on phones 528
call transfer to 467
local 525
monitor-line button 524
personal 527
speeddial.xml file 523, 525
speed-dial command 530
squeeze command 95
srst dn line-mode command 579
srst dn template command 579
srst ephone description command 580
srst ephone template command 579
srst mode auto-provision command 579
SRST using Cisco Unified CME 573
standards 37
supplementary-service h225-notify cid-update (dial-peer) command 252
supplementary-service h225-notify cid-update (voice-service) command 251
supplementary-service h450.12 (dial-peer) command 247
supplementary-service h450.12 (voice-service) command 246
supplementary-service h450.2 (dial-peer) command 244
supplementary-service h450.2 (voice-service) command 243
supplementary-service h450.3 (dial-peer) command 244
supplementary-service h450.3 (voice-service) command 243, 255
supplementary-service h450.3 command 373
supplementary-service h450.7 command 274
supplementary-service qsig call-forward command 274
switchback interval command 211
switchback method command 211
switchover method command 210
system administrator GUI access setup 126
system administrator security token, See SAST
system message command 559
system message display 557

time-format command 66
timeout 355
   busy 355
   interdigit 355
   ringing 355
timeout command 407
timeouts busy command 357
timeouts interdigit (telephony-service) command 357
timeouts ringing (telephony-service) command 357
timers register command 280
time-webedit command 128
time-zone command 62, 66
TLS (transport layer security) 153
toll bar, after-hours 444
toll bar override 444
tone, secondary dial 355
tones, international 62
transcoding support 199
transfer, See call transfer
transfer max-length command 467, 471
transfer-mode command 470
transfer-park blocked command 461
transfer-pattern (telephony-service) command 279, 470
transfer-pattern blocked command 467, 471
transfer-pattern command 242
transfer-system command 67, 241, 279, 466, 469
translate command 120
translation-profile command 120
translation profiles 117
translation rules 117
transport layer security, See TLS
transfer soft key 552
trunk command 268
trunking support 263
trunks, SIP 275
trustpoint 151
trustpoint (credentials) command 186
trustpoint-label command 188
TSP (TAPI Service Provider) software 48

T

TACACS authentication for HTTP server 125
tandem gateways. See H.450 tandem gateways
TAPI (Telephony Application Programming Interface) software 48
telephony-service ccm-compatible (h323 voice-service) command 251
telephony-service ccm-compatible (voice-class) command 252
telephony-service security parameters 173
teleworker remote phones 143
tftp-server-credentials trustpoint command 174
tftp-server flash command 64
TFTP servers
   changing address 57
   storing configuration files 93
three-party conferencing, See conferencing
three-party G.711 conference calls 480
Index

type command 74

U

url command 571
url idle command 559
URL provisioning for customized function buttons 569
user-defined user and network locales 105
user GUI access setup 134
user-locale (ephone-template) command 101, 108
user-locale command 65, 100, 107
user locales 62
  alternative 97
  user-defined 105
username command 135

V

video
  call setup 286
  codec selection process 286
  codecs supported 288
  enabling 291
  endpoints 285
  firmware version 288
  formats supported 288
  icon 289
  phone firmware versions 288
  prerequisites 287
  restrictions 288
  setting parameters 294
  troubleshooting 296
video (config-ephone) command 292
video (config-telephony) command 294
virtual voice port 26
vm-integration command 302
voice mail 299
  Cisco Unity Express integration 300
  Cisco Unity integration 301
  DTMF integration patterns 301
  mailbox selection policy 304
  MWI line selection 519
  MWI prefix specification for SIP 308
  QSIG supplementary services 270
  voice port, virtual 26
  voice translation-profile command 119
  voice translation profiles 117
  voice translation-rule command 119
  voice translation rules 117
  VoIP-to-VoIP connections 224
    configuring 248
    H.450 tandem gateways 231
    hairpin call routing 229

W

web admin customer command 134
web admin system command 127
web customize load command 130

X

XML application programming interface 360
XmlDefault.cnf.xml 92
XML files
  configuration files 91, 291
  downloading xml.template 48
  GUI configuration file 129
  speeddial.xml for system speed dial 523, 525
xml user command 364