CONTENTS

Preface xxvii
  Purpose xxvii
  Audience xxviii
  Organization xxviii
  Related documentation xxix
  Conventions xxix
  Additional information xxxi
  Security overview xxxi

PART I Cisco Unified Communications Manager overview 1

CHAPTER 1 Introduction 3
  Cisco Unified Communications Manager as an Appliance 3
  Benefits 4

CHAPTER 2 Cisco Unified Communications overview 5
  Internet ecosystem 5
  Cisco Unified Communications support 6
    Applications 6
    Call processing 7
    Infrastructure 7
    Clients 7
  Cisco Unified Communications network 8

PART II Cisco Unified Communications Manager system configuration 9

CHAPTER 3 System configuration overview 11
Database replication in a cluster 54
Intercluster communication 55
Balanced call processing 56

CHAPTER 7

Redundancy 59
Cisco Unified Communications Manager redundancy groups 59
Cisco Unified Communications Manager groups 59
Distributing devices for redundancy and load balancing 61
Media resource redundancy 62
CTI redundancy 63

CHAPTER 8

Call admission control 65
Configure locations 66
Configure gatekeeper and gatekeeper-controlled trunk 67
Locations 68
Locations and regions 70
Bandwidth calculations 71
Location-based MLPP 72
Location-based call admission control over intercluster trunk 73
Configure gatekeepers and trunks 74
Components of gatekeeper call admission control 76
Configure gatekeeper and trunk on the router 76
Configure gatekeeper and trunk in Cisco Unified Communications Manager 77

CHAPTER 9

Resource Reservation Protocol 79
Configure RSVP 80
RSVP overview 80
Advantages of RSVP 81
RSVP capabilities 81
RSVP-based MLPP 82
Additional features 83
RSVP caveats 83
RSVP agent and quality of service 83
RSVP agent allocation 84
RSVP agent interaction with location-based CAC 84
### RSVP configuration 85
- Configure clusterwide default RSVP policy 85
- Configure location-pair RSVP policy 85
- Configure RSVP retry 86
- Configure midcall RSVP error handling 87
- Configure MLPP-to-RSVP priority mapping 87

**TSpec 88**
- Audio TSpec 88
- Video TSpec 89

**DSCP 89**

**Application ID 90**

**RSVP for media devices 91**

**Use RSVP between clusters 91**

**Enable RSVP for a call 92**

**Special configuration with RSVP 92**

### Migrate to RSVP 93

### RSVP interactions 94
- RSVP and IPv6 94
- RSVP and shared-line calls 95
- RSVP and music on hold 96
- RSVP and call transfer 97
- RSVP and MLPP 98

### Troubleshooting RSVP 100
- Performance monitoring counters 100
- Call detail records 100
- Alarms 101
- Trace information 101
- Troubleshooting end-to-end RSVP 102

---

### CHAPTER 10 Cisco TFTP 105

- Configure TFTP 106
- TFTP process overview for devices that run SCCP 107
- Configure TFTP for Cisco Unified IP phones that run SIP 107
  - Configuration Sequence for a Phone That Is Running SIP 108
  - Dial Plan Configuration Sequence for a Phone That Is Running SIP 109
Softkey Template Configuration Sequence for a Phone That Is Running SIP 109
Interaction with Cisco Extension Mobility 110
Serviceability Counters 110
Devices that use DHCP and Cisco TFTP 110
TFTP server access for devices that use IPv4 112
TFTP server access for devices that use IPv6 112
Identify the TFTP server for devices 113
Configure a redundant TFTP server 115
Alternate Cisco file servers 115
Centralized TFTP in a multiple cluster environment 116
   Master TFTP server 116
   Send files to the master TFTP server 116
   Centralized TFTP with secure clusters 116
   Configure centralized TFTP 117
Customize and modify configuration files 117

CHAPTER 11
Device support 119
   Supported devices 119
   Device configuration files 120
   Device firmware loads 120
      Update device loads 121
   Device pools 121
   Call preservation 121
      Call preservation scenarios 122

CHAPTER 12
Autoregistration 125
   Configure Autoregistration 125
   Autoregistration overview 126
   Autoregistration with multiple protocol support 127

CHAPTER 13
Dynamic Host Configuration Protocol 129
   DHCP server 129
   Domain Name System 130
   Configure DHCP server 131
   TFTP server device identification 131
### Part III: Dial Plan Architecture

#### Chapter 14: Partitions and Calling Search Spaces

- **Partition and Call Search Spaces** (135)
- **Guidelines and Tips** (137)
- **Dependency Records** (137)
- **Partition Name Limitations** (137)

#### Chapter 15: Time-of-Day Routing

- **Time-of-Day Routing** (139)
  - **Time Periods** (139)
    - **Time Period Behavior** (140)
    - **Time Schedules** (140)
  - **End-Users and Time-of-Day Routing** (141)
  - **Dependency Records** (141)

#### Chapter 16: Understanding Route Plans

- **Automated Alternate Routing** (144)
  - **Automated Alternate Routing Enable Service Parameter** (146)
  - **Automated Alternate Routing and Hunt Pilots** (146)
  - **Automated Alternate Routing and Remote Gateways** (146)
  - **Route Plan Overview** (146)
  - **Route Groups and Route Lists** (147)
  - **Route Patterns** (148)
    - **Route Pattern Usage** (149)
  - **Local Route Groups and Called Party Transformations** (151)
  - **Line Groups** (152)
  - **Hunt Lists** (152)
  - **Hunt Pilots** (152)
  - **Call Coverage** (153)
    - **Hunting and Call Forwarding** (153)
    - **Example of Call Hunting** (153)
CHAPTER 17

Directory numbers 191

Configure directory number 191
Characteristics of directory numbers 192
Shared line appearance 193
Manage directory numbers 197
Directory number features 198
Make and receive multiple calls per directory number 199
<table>
<thead>
<tr>
<th>Chapter</th>
<th>Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>18</td>
<td>Chapter 18: Dial rules overview</td>
</tr>
<tr>
<td></td>
<td>Transfer and conference behavior 200</td>
</tr>
<tr>
<td></td>
<td>Direct transfer and join behavior 200</td>
</tr>
<tr>
<td></td>
<td>Search by directory number 201</td>
</tr>
<tr>
<td></td>
<td>Dependency records 202</td>
</tr>
<tr>
<td></td>
<td><strong>Dial rules overview</strong> 203</td>
</tr>
<tr>
<td></td>
<td>Application dial rules configuration design 203</td>
</tr>
<tr>
<td></td>
<td>Application dial rules configuration error checking 204</td>
</tr>
<tr>
<td></td>
<td>Directory lookup dial rules 205</td>
</tr>
<tr>
<td></td>
<td>SIP dial rules 206</td>
</tr>
<tr>
<td></td>
<td>SIP dial rule patterns 206</td>
</tr>
<tr>
<td></td>
<td>Configure SIP dial rule parameters 207</td>
</tr>
<tr>
<td></td>
<td>Sample Dial Rule for 911 on Cisco Unified IP Phone 7905 207</td>
</tr>
<tr>
<td></td>
<td>Sample Dial Rule for Extension 208</td>
</tr>
<tr>
<td></td>
<td>Private Line Automatic Ringdown (PLAR) 209</td>
</tr>
<tr>
<td>19</td>
<td>Chapter 19: URI dialing</td>
</tr>
<tr>
<td></td>
<td>URI dialing 211</td>
</tr>
<tr>
<td></td>
<td>Set up URI dialing 211</td>
</tr>
<tr>
<td></td>
<td>Directory URI format 213</td>
</tr>
<tr>
<td></td>
<td>Directory URI provisioning 214</td>
</tr>
<tr>
<td></td>
<td>Directory URI and directory number dial string interpretation 214</td>
</tr>
<tr>
<td></td>
<td>Directory URI call routing 215</td>
</tr>
<tr>
<td></td>
<td>Directory URI Replication with ILS 215</td>
</tr>
<tr>
<td></td>
<td>Directory URI interoperability with VCS or third party system 216</td>
</tr>
<tr>
<td></td>
<td>Directory URI LDAP integration 217</td>
</tr>
<tr>
<td></td>
<td>Directory URI and directory number blended address 218</td>
</tr>
<tr>
<td></td>
<td>Set up digit transformations for URI dialing 219</td>
</tr>
<tr>
<td></td>
<td>Directory URI troubleshooting tips 221</td>
</tr>
<tr>
<td></td>
<td><strong>Directory user configuration and credential policy</strong> 223</td>
</tr>
<tr>
<td>20</td>
<td>Chapter 20: Directory overview</td>
</tr>
<tr>
<td></td>
<td>Directory overview 225</td>
</tr>
<tr>
<td></td>
<td>Configure LDAP directory 226</td>
</tr>
<tr>
<td></td>
<td>Cisco Unified Communications Manager and the corporate LDAP directory 227</td>
</tr>
<tr>
<td></td>
<td>Directory access 228</td>
</tr>
</tbody>
</table>
## DirSync service

Configure DirSync service parameters

Authentication

Use the Cisco Unified Communications Manager database

Directory access for Cisco Unified Communications endpoints

### CHAPTER 21

<table>
<thead>
<tr>
<th>Application users and end users</th>
<th>233</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manage application user and end user configuration</td>
<td>233</td>
</tr>
<tr>
<td>Application users</td>
<td>234</td>
</tr>
<tr>
<td>End users</td>
<td>235</td>
</tr>
<tr>
<td>Credential management</td>
<td>236</td>
</tr>
<tr>
<td>User and application profiles</td>
<td>236</td>
</tr>
<tr>
<td>Device association</td>
<td>236</td>
</tr>
<tr>
<td>Device association for application users</td>
<td>236</td>
</tr>
<tr>
<td>Device association for end users</td>
<td>237</td>
</tr>
<tr>
<td>Cisco Unified Mobility for end users</td>
<td>237</td>
</tr>
<tr>
<td>Cisco Extension Mobility profiles</td>
<td>238</td>
</tr>
<tr>
<td>Cisco IP softphone profiles</td>
<td>238</td>
</tr>
</tbody>
</table>

### CHAPTER 22

<table>
<thead>
<tr>
<th>Credential policy</th>
<th>239</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure credential policy</td>
<td>240</td>
</tr>
<tr>
<td>Credential policy and authentication</td>
<td>240</td>
</tr>
<tr>
<td>Credential caching</td>
<td>241</td>
</tr>
<tr>
<td>BAT administration</td>
<td>241</td>
</tr>
<tr>
<td>JTAPI/TAPI support</td>
<td>241</td>
</tr>
<tr>
<td>Credential history</td>
<td>241</td>
</tr>
<tr>
<td>Authentication events</td>
<td>242</td>
</tr>
</tbody>
</table>

### PART V

| Media resources | 243 |

### CHAPTER 23

<table>
<thead>
<tr>
<th>Media resource management</th>
<th>245</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure media resource group and media resource group list</td>
<td>245</td>
</tr>
<tr>
<td>Media resources overview</td>
<td>246</td>
</tr>
<tr>
<td>Trusted relay point</td>
<td>248</td>
</tr>
<tr>
<td>Inter-VRF communication</td>
<td>249</td>
</tr>
</tbody>
</table>
Media firewall traversal 249
Quality-of-Service enforcement 250
Trusted relay point service parameter 250
TRP insertion in Cisco Unified Communications Manager 251
Media resource groups 252
Media resource group lists 253
Dependency records 255

CHAPTER 24
Annunciator 257
Configure annunciator 257
Annunciators overview 258
Secured annunciator through SRTP 259
   Security enabled for annunciator 259
      Secured and non-secured announcements 260
Plan annunciator configuration 261
Annunciator system requirements and limitations 262
Supported tones and announcements 263
Dependency records 264
Annunciator performance monitoring and troubleshooting 264

CHAPTER 25
Conference bridges 265
Configure conference bridge 265
Conference devices overview 266
   Router-based conference capability 266
   Software conference devices 267
   Video conference devices 267
Cisco conference devices (WS-SVC-CMM) 268
MTP WS-X6608 DSP service card 268
Annunciator support for conference bridges 268
Conference bridge types in Cisco Unified Communications Manager administration 268
Conference types 273
   Initiate an ad hoc conference 273
      Ad hoc conference linking 274
      Ad hoc conference settings 276
Drop ad hoc conference 277
Enable advanced ad hoc conference 278
Enable non-linear ad hoc conference linking 278
Ad hoc conference settings restrictions for phones that are running SIP 279
Ad hoc conference limitations 280
Meet-me conference 280
Meet-me conference limitations 280
Conferences and the party entrance tone 280
Intelligent bridge selection 281
Configure intelligent bridge selection 282
Choose encrypted audio conference Instead of video conference 282
Minimum video-capable participants to allocate video conference 283
Allocate video conference bridge for audio-only conferences when video conference
bridge has higher priority 283
Limitations of intelligent bridge selection 283
Blind conference over SIP ICT 283
Conference over H323 ICT 284
Dependency records 284
Conference bridge performance monitoring and troubleshooting 285

CHAPTER 26  Transcoders  287
Configure transcoder  287
Transcoders overview  288
Manage transcoders with the Media Resource Manager  288
Use transcoders as MTPs  288
Transcoders and call throttling  289
Transcoder types in Cisco Unified Communications Manager administration  289
Transcoder failover and fallback  291
Active Cisco Unified Communications Manager becomes inactive  291
Reset registered transcoder devices  291
Dependency records  292
Transcoder performance monitoring and troubleshooting  292

CHAPTER 27  Music on hold  293
CHAPTER 28

**Media Termination Points** 295

Configure software MTP 295

Media Termination Points overview 296

Manage MTPs with the Media Resource Manager 297

MTPs and Call Throttling 297

MTP types in Cisco Unified Communications Manager administration 298

Plan software MTP 298

  Software MTP device characteristics 299

  Avoid call failure 299

MTP system requirements and limitations 300

MTP failover and fallback 300

  Active Cisco Unified Communications Manager becomes inactive 300

  Reset registered MTP devices 300

Dependency records 301

Software MTP performance monitoring and troubleshooting 301

CHAPTER 29

**Cisco DSP resources for transcoding conferencing and MTP** 303

Cisco DSP resources 303

  Hardware-based MTP transcoding services 304

    IP-to-IP packet transcoding and voice compression 305

    Voice compression IP-to-IP packet transcoding and conferencing 305

    IP-to-IP packet transcoding across intercluster trunks 306

  Hardware-based conferencing services 306

Supported Cisco Catalyst gateways and Cisco Access routers 307

  Cisco Catalyst 4000 WS-X4604-GWY 307

  Cisco Catalyst 6000 WS-6608-T1 or WS-6608-E1 308

  Cisco 2600 Cisco 2600XM Cisco 2800 Cisco 3600 Cisco 3700 Cisco 3800 and Cisco

    VG200 for NM-HDV 309

  Cisco 2600XM Cisco 2691 Cisco 2800 Cisco 3600 Cisco 3700 and Cisco 3800 for

    NM-HD and NM-HDV2 310

PART VI

**Voice Mail and messaging integration** 313

CHAPTER 30

**Voice Mail connectivity to Cisco Unified Communications Manager** 315
Contents

CHAPTER 31 SMDI Voice Mail integration 325
   Configure SMDI 325
   SMDI voice messaging integration requirements 326
   Configure port for SMDI 327
   Cisco Messaging Interface redundancy 327

CHAPTER 32 Cisco Unity Messaging integration 331
   Set up Cisco Unity and Cisco Unity connection 331
   System requirements 332
   Integration description 333
   Cisco Unified Communications Manager SIP trunk integration 334
   Secure the Voice Mail port 334

CHAPTER 33 Cisco DPA integration 335
   DPA 7630/7610 335
   DPA 7630/7610 overview 336
      When to use the DPA 7630/7610 336
      When to use SMDI 336
      When not to use SMDI 337

PART VII System features 339

CHAPTER 34 Call Park and Directed Call Park 341

CHAPTER 35 Call Pickup 343
CHAPTER 36  Cisco Unified IP phone services 345
  Configure Cisco Unified IP phone service 345
  Cisco Unified IP phone services overview 347
  Installation and upgrade considerations for IP phone services 348
  Phone support for IP phone services 348
  Guidelines and tips 349
  Dependency records 349

CHAPTER 37  Cisco Extension Mobility and phone login features 351

CHAPTER 38  Cisco Unified Communications Manager Assistant 353

PART VIII  Devices and protocols 355

CHAPTER 39  Cisco Unified Communications Manager voice gateways overview 357
  Set up gateway 357
  Set up MGCP BRI gateway 358
  Cisco voice gateways 359
    Standalone voice gateways 360
      Cisco VG248 Analog Phone Gateway 360
      Cisco VG224 Analog Phone Gateway 361
      Cisco Voice Gateway 200 361
    MGCP BRI call connections 362
    Switch-based gateways 363
      Cisco Catalyst 6000 8-Port Voice T1/E1 and Services Module 363
      Cisco Catalyst 6000 24 Port FXS Analog Interface Module 363
      Cisco Communication Media Module 364
      Cisco Catalyst 4000 Access Gateway Module 364
      Cisco Catalyst 4224 Voice Gateway Switch 364
    H.323 Gateways 365
      Cisco IOS H.323 Gateways 365
      Outbound FastStart call connections 365
    Voice gateway model summary 365
  Gateways dial plans and route groups 374
Dependency records for gateways and their route groups and directory numbers 375
Gateways and the Local Route Groups feature 375
Gateways and the Calling Party Normalization feature 375
Apply the international escape character to inbound calls over H.323 trunks 376
Gateway failover and fallback 376
MGCP gateways 377
IOS H.323 gateways 377
Cisco VG248 Analog Phone Gateway 378
Transfer calls between gateways 378
Transfer capabilities using gateway configuration 378
Set up transfer capabilities by using Call Classification service parameter 379
Block transfer capabilities by using service parameters 379
H.235 support for gateways 380

CHAPTER 40
IP telephony protocols 381
IP protocols 381
H.323 Protocol 381
Media Gateway Control Protocol (MGCP) 382
Skinny Client Control Protocol (SCCP) 382
Session Initiation Protocol (SIP) 382
Analog telephony protocols 383
Loop-Start Signaling 383
Ground-Start Signaling 383
E&M Signaling 384
Channel Associated Signaling (CAS) 384
T1 CAS 385
E1 CAS 385
Digital telephony protocols 385
Basic Rate Interface (BRI) 385
T1 Primary Rate Interface (T1 PRI) 385
E1 Primary Rate Interface (E1 PRI) 386
Q. Signaling (QSIG) 386
Annex M.1 (message tunneling for QSIG) 387
QSIG tunneling over SIP trunk 387
Basic call for QSIG 389
<table>
<thead>
<tr>
<th>Feature</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Call completion</td>
<td>389</td>
</tr>
<tr>
<td>Call diversion</td>
<td>389</td>
</tr>
<tr>
<td>Call transfer</td>
<td>390</td>
</tr>
<tr>
<td>Compatibility with older versions of QSIG Protocol (ECMA)</td>
<td>391</td>
</tr>
<tr>
<td>Facility selection and reservation</td>
<td>391</td>
</tr>
<tr>
<td>Identification services</td>
<td>392</td>
</tr>
<tr>
<td>Message Waiting Indication (MWI) service</td>
<td>393</td>
</tr>
<tr>
<td>Path replacement</td>
<td>394</td>
</tr>
<tr>
<td>QSIG interface to Cisco Unified Communications Manager</td>
<td>395</td>
</tr>
</tbody>
</table>

**CHAPTER 41: Session Initiation Protocol**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP trunk configuration</td>
<td>397</td>
</tr>
<tr>
<td>SIP phone configuration</td>
<td>397</td>
</tr>
<tr>
<td>SIP networks</td>
<td>398</td>
</tr>
<tr>
<td>SIP and Cisco Unified Communications Manager</td>
<td>398</td>
</tr>
<tr>
<td>Media Termination Point (MTP) devices</td>
<td>399</td>
</tr>
<tr>
<td>Configure regions for SIP devices with the MTP required option enabled</td>
<td>400</td>
</tr>
<tr>
<td>SIP service parameters</td>
<td>400</td>
</tr>
<tr>
<td>SIP Interoperability</td>
<td>400</td>
</tr>
<tr>
<td>SIP timers and counters</td>
<td>400</td>
</tr>
<tr>
<td>Supported audio media types</td>
<td>402</td>
</tr>
<tr>
<td>Supported video media types</td>
<td>403</td>
</tr>
<tr>
<td>Supported application media type</td>
<td>403</td>
</tr>
<tr>
<td>Supported T38 fax payload type</td>
<td>403</td>
</tr>
<tr>
<td>SIP profiles for trunks</td>
<td>404</td>
</tr>
<tr>
<td>SIP trunk security profiles</td>
<td>404</td>
</tr>
<tr>
<td>SIP UDP port throttling</td>
<td>404</td>
</tr>
<tr>
<td>SIP trunks between releases of Cisco Unified CallManager and Cisco Unified Communications Manager</td>
<td>405</td>
</tr>
<tr>
<td>SIP forking for SIP trunk</td>
<td>406</td>
</tr>
<tr>
<td>SIP transparency and normalization</td>
<td>407</td>
</tr>
<tr>
<td>Tracing for SIP normalization</td>
<td>408</td>
</tr>
<tr>
<td>Alarms for SIP normalization</td>
<td>409</td>
</tr>
<tr>
<td>Performance counters for SIP normalization</td>
<td>409</td>
</tr>
<tr>
<td>Dependency records</td>
<td>410</td>
</tr>
</tbody>
</table>
SIP functions that are supported in Cisco Unified Communications Manager 410

Basic calls between SIP endpoints and Cisco Unified Communications Manager 410

Basic outgoing call 410
Basic incoming call 410
Use of early media 410

DTMF relay calls between SIP endpoints and Cisco Unified Communications Manager 411

Forward DTMF digits from SIP devices to gateways or Interactive Voice Response (IVR) systems for dissimilar DTMF methods 411
Generate DTMF digits for dissimilar DTMF methods 411

Supplementary services that are initiated if an MTP is allocated 412
Ringback tone during blind transfer 412

Supplementary services that are initiated by SIP endpoint 413
SIP-initiated call transfer 413
Call hold 413
Call forward 413

Enhanced Call Identification services 413
Call line and name identification presentation 414
Call line and name identification restriction 414
SIP CLI Handling Change 415
Connected line and name identification presentation 416
Connected line and name identification restriction 417

Redirecting Dial Number Identification Service (RDNIS) 417

Redirect 417
Support of G. Clear codec for SIP trunks 418
Early offer for G.Clear calls 420

Support of Multilevel Precedence and Preemption for SIP trunks 420
Resource Priority Namespace Network Domains 420

Support for secure V.150.1 Modem over IP over SIP trunks 421
Support for G.729a and G.729b codecs over SIP trunks 421
Support for SIP T.38 interoperability with Microsoft Exchange 422
Support for QSIG tunneling over SIP 422

SIP PUBLISH 422
Cisco Unified Communications Manager and Cisco Unified Presence high-level architecture overview 423
SIP OPTIONS 426
SIP early offer 429
   Early offer limitations and interactions 431
   Traces 433
   Troubleshooting early offer issues 435
Cisco Unified Communications Manager SIP endpoints overview 438
SIP line side overview 440
SIP standards 440
   RFC3261 RFC3262 (PRACK) RFC3264 (offer/answer) RFC3311 (UPDATE)
   3PCC 440
   RFC3515 (REFER) also replaces and referred-by headers 440
Remote Party Id (RPID) header 441
Diversion header 441
Replaces header 441
Join header 441
P-Charging-Vector header 441
RFC3265 + Dialog Package 442
RFC3265 + Presence Package 442
RFC3265 + KPML Package 442
RFC3265 + RFC3842 MWI Package (unsolicited notify) 442
Remotecc 442
RFC4028 session timers 443
Cisco Unified Communications Manager functionality that is supported by phones that are
running SIP 443
Dial plans 443
Do not disturb 443
PLAR 443
Softkey handling 443
DSCP configuration 444
SIP profiles for endpoints 444
Network Time Protocol (NTP) 444
CTI support 445
Single button Barge/cBarge 445
Join and Join Across Lines 445
Programmable line keys 445
Malicious Call Identification (MCID) 445
Single call UI 446
Directed Call Pickup 446
Unified Mobile Communications Server (UMCS) integration 446
Do Not Disturb (DND) Call Reject 446
BLF Call Pickup 446
Calling party normalization 447
E.164 447
Soft client dual registration 447

CHAPTER 42

Cisco Unified Communications Manager trunk types 449
Set up SIP trunk 449
Cisco Unified Communications Manager trunk configuration 451
Trunks and gatekeepers in Cisco Unified Communications Manager 451
Gatekeeper-controlled trunks 451
Non-gatekeeper-controlled trunks 452
Trunk types in Cisco Unified Communications Manager administration 452
H.225 trunk (gatekeeper controlled) 452
Intercluster trunk (gatekeeper controlled) 453
Intercluster trunk (non-gatekeeper controlled) 453
SIP trunk 453
Trunks and the Calling Party Normalization feature 454
Apply the international escape character to inbound calls over H.323 trunks 455
Transfer calls between trunks 456
Transfer capabilities using trunk configuration 456
Set up transfer capabilities by using Call Classification service parameter 457
Block transfer capabilities by using service parameters 457
Dependency records for trunks and associated route groups 458
H.235 support for trunks 458

CHAPTER 43

Cisco Unified IP phones 459
Phone configuration 460
Configure phone for SCCP 460
Configure phone for SIP 461
Supported Cisco Unified IP phones 462
Third-party SIP endpoints 479
H.323 clients and CTI ports 479
CTI remote device setup 480
Client Services Framework setup 484
Cisco IP Communicator 500
Cisco Unified Personal Communicator 500
Cisco TelePresence 501
Cisco Unified Mobile Communicator 501
Codec usage 501
Phone button templates 503
  Default phone button templates 504
  Guidelines for customizing phone button templates 509
Programmable line keys 512
Softkey templates 514
  Add application 515
  Configure softkey layout 516
Softkey template operation 517
Common phone profiles 518
Methods for adding phones 518
Phone migration 519
Phone features 520
  Agent Greeting 520
  Audible Message Waiting Indicator (AMWI) 520
  Barge and Privacy 521
  Calling Party Normalization 521
  Call Forward 521
  Call Waiting 524
  Cancel Call Waiting 524
  Call Diagnostics and Voice-Quality Metrics 525
  Call Park 525
  Call Pickup 525
  Call Pickup Notification 526
  Call Select 526
  Conference Linking 526
  Conference List 527
CHAPTER 44

Video telephony 543

Configure video telephony 543
Introducing video telephony 544

Video calls 545
Real-Time Transport Control Protocol pass-through 545
Video codecs 546
Video network 547
Enabling an audio-only device with video 548
H.323 video 549
Dynamic H.323 addressing 549
  Registering with the gatekeeper 549
  Call processing 550
  Configuration notes 550
H.239-Extended video channels in H.323 call 551
  Support for third-party H.323 devices 551
  H.323 devices invoke presentation feature 551
  Opening second video channels 552
  Call Admission Control (CAC) on second video channels 553
  Number of video channels allowed 554
  H.239 commands and indication messages 554
  Topology and protocol interoperability limitation 554
  Midcall feature limitation 554
Skinny client control protocol video 555
Skinny client control protocol video bridging 555
Video over Wi-Fi 555
Video for SNR call 555
SIP video 556
  Configuring SIP devices for video calls 556
Cisco video conference bridges 557
  Cisco TelePresence MCU video conference bridge 557
  Cisco Unified MeetingPlace video conference bridge 558
  ISR G2 Router video conference bridge 559
Cisco TelePresence Video Communications Server 560

Configure interoperability with Cisco TelePresence Video Communications Server 560

Video encryption 561

Encryption methods 561
Negotiation of the encryption method 562
Supported protocols 563

Endpoint support for the Binary Floor Control Protocol 563

Presentation sharing with the Binary Floor Control Protocol 565

BFCP configuration tips 566
BFCP limitations 567
Supported features with BFCP 567

Bandwidth management 568

Call Admission Control 568
Session level bandwidth modifiers 569
RSVP 569
Alternate routing 570
DSCP marking 570

Phone configuration for video calls 570
Additional configuration for video calls 570

Trunk interaction with H.323 client 571
Call routing for video calls 571
Gateway timer parameter 571

Conference control for video conferencing 571

Video and interoperability 572

Protocols and deployments 572
Cisco and third-party endpoints supported 572
Limitations 573
Internet Protocol Version 6 (IPv6) 573

Far End Camera Control protocol support 574

Video telephony and Cisco Unified Serviceability 574

Performance monitoring counters 574
Video bridge counters 575
Call Detail Records 575
CHAPTER 45  Computer Telephony Integration 577

Configure CTI 577
Computer Telephony Integration applications 578
CTIManager 579
Media Termination Points 580
CTI-controlled devices 580
User management and CTI controlled devices 582
Applications that monitor and control all CTI-controllable devices 583
IPv6 and CTI 584
Dependency records 584
CTI redundancy 584
Cisco Unified Communications Manager 584
CTIManager 585
Application failure 585

CHAPTER 46  Cisco ATA 186 587

Configure Cisco ATA 587
Cisco ATA 186 features 587
Connecting with Cisco Unified Communications Manager 588

CHAPTER 47  Administrative tools overview 589

Bulk Administration Tool (BAT) 589
Cisco Unified Serviceability 589
CDR Analysis and Reporting (CAR) 590
Call Detail Records 590
Preface

This preface describes the purpose, audience, organization, and conventions of this guide and provides information on how to obtain related documentation.

Note

This document may not represent the latest Cisco product information available. You can obtain the most current documentation by accessing Cisco's product documentation page at this URL:

- Purpose, page xxvii
- Audience, page xxviii
- Organization, page xxviii
- Related documentation, page xxix
- Conventions, page xxix
- Additional information, page xxxi
- Security overview, page xxxi

Purpose

The Cisco Unified Communications Manager System Guide provides conceptual information about Cisco Unified Communications Manager (formerly Cisco Unified CallManager) and its components as well as tips for setting up features by using Cisco Unified Communications Manager Administration. This book acts as a companion to the Cisco Unified Communications Manager Administration Guide, which provides instructions for administering the Cisco Unified Communications Manager system, including descriptions of procedural tasks that you complete by using Cisco Unified Communications Manager Administration.
**Audience**

The Cisco Unified Communications Manager System Guide provides information for network administrators who are responsible for managing the Cisco Unified Communications Manager system. This guide requires knowledge of telephony and IP networking technology.

**Organization**

The following table shows the organization of this guide:

<table>
<thead>
<tr>
<th>Part</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Part 1</td>
<td>“Understanding Cisco Unified Communications Manager”</td>
</tr>
<tr>
<td></td>
<td>Provides an overview of Cisco Unified Communications Manager and Cisco Unified Communications network components.</td>
</tr>
<tr>
<td>Part 2</td>
<td>“Understanding Cisco Unified Communications Manager System Configuration”</td>
</tr>
<tr>
<td></td>
<td>Details the basic configuration flow for a Cisco Unified Communications Manager system and explains system-level configuration concepts and settings.</td>
</tr>
<tr>
<td>Part 3</td>
<td>“Dial Plan Architecture”</td>
</tr>
<tr>
<td></td>
<td>Describes route plans, partitions, calling search spaces, time-of-day routing, directory numbers, and dial rules.</td>
</tr>
<tr>
<td>Part 4</td>
<td>“Directory, User Configuration, and Credential Policy”</td>
</tr>
<tr>
<td></td>
<td>Provides information about the directory, application users, end users, and credential policy.</td>
</tr>
<tr>
<td>Part 5</td>
<td>“Media Resources”</td>
</tr>
<tr>
<td></td>
<td>Explains how to manage and configure media resources such as transcoders, annunciators, conference bridges, media termination points, music on hold audio sources, and music on hold servers.</td>
</tr>
<tr>
<td>Part 6</td>
<td>“Voice Mail and Messaging Integration”</td>
</tr>
<tr>
<td></td>
<td>Discusses how to integrate voice mail and messaging solutions with Cisco Unified Communications Manager.</td>
</tr>
<tr>
<td>Part 7</td>
<td>“System Features”</td>
</tr>
<tr>
<td></td>
<td>Describes additional system-wide features such as call park, call pickup, and Cisco Unified IP Phone services.</td>
</tr>
<tr>
<td>Part 8</td>
<td>“Devices and Protocols”</td>
</tr>
<tr>
<td></td>
<td>Explains how to configure supported voice gateways, protocols, Cisco Unified IP Phones, video telephony, and software applications for Cisco Unified Communications Manager.</td>
</tr>
</tbody>
</table>
Related documentation

See the following documents for further information about related Cisco Unified Communications applications and products:

- Installing Cisco Unified Communications Manager Release 8.6(1)
- Upgrading Cisco Unified Communications Manager Release 8.6(1)
- Cisco Unified Communications Manager Documentation Guide
- Release Notes for Cisco Unified Communications Manager Release 8.6(1)
- Cisco Unified Communications Manager Administration Guide
- Cisco Unified Communications Manager Features and Services Guide
- Cisco Unified Serviceability Administration Guide
- Cisco Unified Communications Manager Call Detail Records Administration Guide
- Cisco Unified Real-Time Monitoring Tool Administration Guide
- Troubleshooting Guide for Cisco Unified Communications Manager
- Cisco Unified IP Phone Administration Guide for Cisco Unified Communications Manager
- Cisco Unified Communications Manager Bulk Administration Guide
- Cisco Unified Communications Manager Security Guide
- Cisco Unified Communications Solution Reference Network Design (SRND)

Conventions

This document uses the following conventions:

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>boldface</strong></td>
<td>Commands and keywords are in <strong>boldface</strong>.</td>
</tr>
<tr>
<td><em>italic</em></td>
<td>Arguments for which you supply values are in <em>italics</em>.</td>
</tr>
<tr>
<td>[ ]</td>
<td>Elements in square brackets are optional.</td>
</tr>
<tr>
<td>{ x</td>
<td>y</td>
</tr>
<tr>
<td>Convention</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-------------</td>
</tr>
<tr>
<td>[ x</td>
<td>y</td>
</tr>
<tr>
<td>string</td>
<td>A non-quoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.</td>
</tr>
<tr>
<td>screen font</td>
<td>Terminal sessions and information the system displays are in screen font.</td>
</tr>
<tr>
<td>screen font</td>
<td>Information you must enter is in screen font.</td>
</tr>
<tr>
<td>italic screen font</td>
<td>Arguments for which you supply values are in italic screen font.</td>
</tr>
<tr>
<td>^</td>
<td>The symbol ^ represents the key labeled Control-for example, the key combination ^D in a screen display means hold down the Control key while you press the D key.</td>
</tr>
<tr>
<td>&lt;&gt;</td>
<td>Nonprinting characters, such as passwords, are in angle brackets.</td>
</tr>
</tbody>
</table>

Notes use the following conventions:

**Note**
Means reader take note. Notes contain helpful suggestions or references to material not covered in the publication.

Timesavers use the following conventions:

**Timesaver**
Means the described action saves time. You can save time by performing the action described in the paragraph.

Tips use the following conventions:

**Tip**
Means the information contains useful tips.

Cautions use the following conventions:

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

Warnings use the following conventions:
This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, you must be aware of the hazards involved with electrical circuitry and familiar with standard practices for preventing accidents.

Additional information

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly What's New in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at:


Subscribe to the What's New in Cisco Product Documentation as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

Security overview

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

Further information regarding U.S. export regulations may be found at http://www.access.gpo.gov/bis/ear/ear_data.html.
Cisco Unified Communications Manager overview

- Introduction, page 3
- Cisco Unified Communications overview, page 5
Introduction

This chapter provides information about the Cisco Unified Communications Manager (formerly Cisco Unified CallManager) which serves as the software-based, call-processing component of Cisco Unified Communications. The Cisco Unified Communications Applications Server provides a high-availability server platform for Cisco Unified Communications Manager call processing, services, and applications.

The Cisco Unified Communications Manager system extends enterprise telephony features and functions to packet telephony network devices such as IP phones, media processing devices, voice-over-IP (VoIP) gateways, and multimedia applications. Additional data, voice, and video services, such as unified messaging, multimedia conferencing, collaborative contact centers, and interactive multimedia response systems, interact through Cisco Unified Communications Manager open telephony application program interface (API).

Cisco Unified Communications Manager provides signaling and call control services to Cisco integrated telephony applications as well as to third-party applications. It performs the following primary functions:

- Call processing
- Signaling and device control
- Dial plan administration
- Phone feature administration
- Directory services
- Operations, administration, management, and provisioning (OAM&P)
- Programming interface to external voice-processing applications such as Cisco IP Communicator, Cisco Unified IP Interactive Voice Response (IP IVR), and Cisco Unified Communications Manager Attendant Console

- Cisco Unified Communications Manager as an Appliance, page 3
- Benefits, page 4

Cisco Unified Communications Manager as an Appliance

Cisco Unified Communications Manager works as an Appliance on a non-Windows-based Operating System. The Cisco Unified Communications Manager appliance refers to the following functions:
• Works on a specific hardware platform(s) that Cisco specifies and supplies and, in some cases, the customer supplies
• Works in a carefully controlled software environment that Cisco specifies and installs
• Includes all software that is required to operate, maintain, secure, and manage servers
• Outputs a variety of management parameters via a published interface to provide information to approved management applications such as, but not limited to, NetIQ Vivinet Manager, HP Openview, and Integrated Research Prognosis
• Operates in a headless manner (without keyboard, mouse, or VGA monitor support) or (in the case of some of the hardware platforms) in a headed manner (with keyboard, mouse, and monitor)

Exposed interfaces
  ◦ Ethernet to the network
  ◦ Web interface for Platform and Cisco Unified Communications Manager Administration
  ◦ Command Line Interface (CLI) based platform shell for administrator use
  ◦ APIs such as JTAPI, AXL/SOAP, and SNMP for third-party application and management support

• Cisco Unified Communications Manager servers get preinstalled with software to ease customer and partner deployment and automatically search for updates and notify administrators when key security fixes and software upgrades are available for their system. This process comprises Electronic Software Delivery.
• You can upgrade Cisco Unified Communications Manager servers while they continue to process calls, so upgrades take place with minimal downtime.
• Cisco Unified Communications Manager supports the Asian and Middle Eastern markets by providing support for Unicode on higher resolution phone displays.
• Cisco Unified Communications Manager provides Fault, Configuration, Accounting, Performance, and Security (FCAPS).

Benefits

The Cisco Unified Communications Manager system includes a suite of integrated voice applications that perform voice conferencing and manual attendant console functions. Supplementary and enhanced services such as hold, transfer, forward, conference, multiple-line appearances, automatic route selection, speed dial, last-number redial, and other features extend to IP phones and gateways. Because Cisco Unified Communications Manager is a software application, enhancing its capabilities in production environments requires only upgrading software on the server platform, thereby avoiding expensive hardware upgrade costs. Distribution of Cisco Unified Communications Manager and all Cisco Unified IP Phones, gateways, and applications across an IP network provides a distributed, virtual telephony network. This architecture improves system availability and scalability. Call admission control ensures that voice quality of service (QoS) is maintained across constricted WAN links and automatically diverts calls to alternate public switched telephone network (PSTN) routes when WAN bandwidth is not available.

A web-browsable interface to the configuration database provides the capability for remote device and system configuration. This interface also provides access to HTML-based online help for users and administrators.
Cisco Unified Communications overview

This chapter provides information about Cisco Unified Communications. Multiple communication networks exist as entirely separate entities, each serving a specific application. The traditional public switched telephone network (PSTN) time-division multiplexing (TDM) network serves the voice application; the Internet and intranets serve data communications.

Business requirements often force these networks to interoperate. As a result, deploying multiservice (data, voice, and video) applications such as unified messaging or web-based customer contact centers requires expensive and complex links between proprietary systems, such as private branch exchanges (PBXs) and standards-based data networks.

The traditional enterprise communication takes place on two separate networks:

- Voice
- Data

- Internet ecosystem, page 5
- Cisco Unified Communications support, page 6
- Cisco Unified Communications network, page 8

Internet ecosystem

Over time, the Internet (and data networking technology in general) encompassed the traditional traffic types. This convergence recently started to absorb voice and video as applications into the data network. Several large Post, Telephone, and Telegraph (PTT) carriers use packet switching or voice over ATM as their backbone technology, and enterprise customers accept virtual trunking, or connect their disparate PBXs via their wide-area data network, to avoid long-distance charges.

Converging these previously disparate networks into a single, unified network realizes savings in multiple areas, including lower total cost of ownership, toll savings, and increased productivity.

Cisco Unified Communications Manager (formerly Cisco Unified CallManager) and Cisco Unified IP Phones provide an IP telephony solution that operates on an IP infrastructure.

The clustering architecture of Cisco Unified Communications Managers allows you to scale to a highly available voice-over-IP (VoIP) network.
Cisco Unified Communications support

Cisco Unified Communications support encompasses the following components:

- Converged client devices
- Hardware/software
- Directory services
- Call processing
- Telephony/data applications
- Network management
- Service and support

Cisco Unified Communications solutions enable you to

- Deploy IP-enabled business applications
- Implement a standards-based open architecture
- Migrate to a converged network in your own time frame

Cisco Unified Communications support enables you to move from maintaining a separate data network and a closed, proprietary voice PBX system to maintaining one open and standards-based, converged network for all your data, voice, and video needs.

Applications

The following list includes the major Cisco Unified Communications voice and video applications:

- Cisco Unified Communications Manager-This software-only call-processing application distributes calls, features, phones, regions, and groups over an IP network.
- Cisco Unity-The Cisco Unity messaging application provides voice messaging to enterprise communications.
- Cisco Unity Connection-For more information about Cisco Unity Connection, see the applicable Cisco Unified Communications Manager SCCP Integration Guide for Cisco Unity Connection or the Cisco Unified Communications Manager SIP Trunk Integration Guide for Cisco Unity Connection.
- Video-IP-TV and IP-video conferencing products enable distance learning and workgroup collaboration.
- Cisco Unified IP-IVR-As an IP-powered interactive voice response (IVR) solution, Cisco Unified IP-IVR, combined with Cisco IP Auto-Attendant, provides an open and feature-rich foundation for delivering IVR solutions over an IP network.
- Cisco IP Communicator-The Cisco IP Communicator, a software, computer-based phone, provides communication capabilities that increase efficiency and promote collaboration.
Call processing

Cisco Unified Communications Manager, a software-only call-processing application, distributes calls and features and provides scalability.

Cisco Unified Communications Manager provides signaling and call-control services to Cisco-integrated applications, as well as to third-party applications.

Infrastructure

The following list shows the components of the infrastructure layer of Cisco Unified Communications:

- Media convergence servers
- General voice products for Cisco Unified Communications Solutions
- Switches
- Integrated IP telephony solution
- Voice trunks
- Voice gateways
- Toll bypass products
- IP protocols such as MGCP, H.323, and SIP

Clients

Cisco delivers the following IP-enabled communication devices:

- Cisco Unified IP Video Phone 7985-supports SCCP
- Cisco Unified IP Phone 7975-supports SCCP and SIP
- Cisco Unified IP Phone 7970/7971-supports SCCP and SIP
- Cisco Unified IP Phone 7962/7965-supports SCCP and SIP
- Cisco Unified IP Phone 7960/7961-supports SCCP and SIP
- Cisco Unified IP Phone 7942/7945-supports SCCP and SIP
- Cisco Unified IP Phone 7940/7941-supports SCCP and SIP
- Cisco Unified IP Phone 7931-supports SCCP
- Cisco Unified Wireless IP Phone 7921-supports SCCP
- Cisco Unified Wireless IP Phone 7920-supports SCCP
- Cisco Unified IP Phone 7912-supports SCCP and SIP
- Cisco Unified IP Phone 7911-supports SCCP and SIP
- Cisco Unified IP Phone 7910-supports SCCP
- Cisco Unified IP Phone 7906-supports SCCP and SIP
Cisco Unified Communications network

- Cisco Unified IP Phone 7905—supports SCCP and SIP
- Cisco Unified IP Phone 7902—supports SCCP
- Cisco Unified IP Conference Station 7936
- Cisco Unified IP Conference Station 7935
- Cisco IP Communicator
- Cisco Unified IP Phone Expansion Module 7914/7915/7916

Cisco also supports various third-party phones that are running SIP. Contact your Cisco representative for more information.

Cisco Unified Communications network

The Cisco Unified Communications network includes the following components:

- Cisco Unified Communications Manager
- Cisco Unified IP Phones
- IOS platforms
- Power Over Ethernet (POE) switches
- Digital gateways and trunks
- Analog gateways
- Transcoders
- Conferencing (hardware/software)
- Media Termination Point (MTP)
- Music On Hold (MOH)
- Annunciator
- Inline power modules (10/100 Ethernet switching modules)
- Cisco IP Communicator

Control from the Cisco Unified IP Phone to Cisco Unified Communications Manager uses SCCP client control protocol and, independently, desktop computer to Cisco Unified Communications Manager, as an H.323 gatekeeper that is using H.225/H.245 over transmission control protocol (TCP).
Cisco Unified Communications Manager system configuration

• System configuration overview, page 11
• Roles and user groups, page 15
• System-level configuration settings, page 29
• Clustering, page 53
• Redundancy, page 59
• Call admission control, page 65
• Resource Reservation Protocol, page 79
• Cisco TFTP, page 105
• Device support, page 119
• Autoregistration, page 125
• Dynamic Host Configuration Protocol, page 129
System configuration overview

This chapter provides information about the overall flow, or order, for configuring the components of your Cisco Unified Communications network.

For best results when you are configuring a complete Cisco Unified Communications system, start with the system-level components and work toward the individual devices. For example, you must configure the appropriate device pools, route lists, locations, and calling search spaces before you can use those components to configure phones and lines.

- Configure system, page 11

Configure system

The general steps that are involved in configuring a complete IP telephony system are as follows. If you are not using a particular feature or component, you can skip that step. You have some flexibility in the order for performing these configuration steps, and in some cases, you might have to alternate between steps or return to a given step several times to complete your configuration.

Procedure

**Step 1**
Install the Cisco Unified Communications Manager software on one server. This server acts as the database server.

**Step 2**
Activate services, as required, on the database server.

**Step 3**
Configure system-level settings:

- Cisco Unified Communications Managers (Be aware that some Cisco Unified Communications Manager-specific elements, such as enabling of auto-registration and establishing a starting directory number [DN], are required.)
- Date/time groups
- Regions
- Softkey templates (Softkey templates represent a required field in device pool configuration, but they offer standard template options as well.)
- Device defaults
• Enterprise parameters
• Locations

Step 4  Design and configure your dialing plan:
• AAR Group
• Application Dial Rules (optional, used by Cisco Unified Communications Manager Assistant and Cisco Web Dialer)
• Partitions
• Calling search spaces
• Route filters
• Route groups and line groups
• Route and hunt lists
• Route patterns (If you want to assign route patterns to gateways, you need to create gateways prior to configuring the route pattern for those gateways.)
• Translation patterns

Step 5  Configure media resources:
• Conference bridges
• Transcoders
• Annunciator
• Media termination points
• Music on hold audio sources
• Music on hold servers
• Media resource groups
• Media resource group lists

Step 6  Configure device pool settings:
• Cisco Unified Communications Manager group
• Date/Time group
• Regions
• Softkey template
• SRST reference
• Calling Search Space for Auto-registration
• Media Resource Group List
• Network Hold MOH Audio Source
• User Hold MOH Audio Source
• Network Locale
• User Locale

Step 7  Install and configure the following voice-messaging systems:
   • Cisco Unity Connection voice-messaging system

Step 8  Configure meet-me numbers/patterns.
Step 9  Configure message-waiting numbers.
Step 10 Configure features such as
   • Call park/Directed call park
   • Call pickup, group call pickup, other group pickup, directed call pickup, and busy lamp field (BLF) call pickup
   • Barge
   • Immediate Divert
   • Cisco Unified IP Phone services
   • Cisco Extension Mobility

Step 11 Install and configure the gateways.
Step 12 Add end users through Cisco Unified Communications Manager Administration (when synchronization with an LDAP server is not enabled).
   Manage credentials for end users.
   Create Cisco Unity Connection voice mailboxes.
Step 13 Configure and install the phones; then, associate users with the phones. Also, configure phone button templates and softkey templates.
Step 14 Enable computer telephony integration (CTI) application support; then, install and configure the desired CTI applications.
Roles and user groups

This chapter provides information about roles and user groups in Cisco Unified Communications Manager Administration which uses roles and user groups to provide varying levels of privilege (access). This technique permits granting only the required privileges for a selected group of users and limits the configuration functions that users in a particular user group can perform.

- Overview, page 15
- Roles, page 16
- User groups, page 25
- Access log, page 26
- Enterprise parameters, page 26
- Create a custom help desk role and user group, page 26

Overview

Roles and user groups provide multiple levels of security to Cisco Unified Communications Manager Administration and to other applications. The system groups the resources that are available to Cisco Unified Communications Manager Administration and to other applications into roles. Each application comes with standard, predefined roles. Each application defines its own access privilege for Cisco Unified Communications Manager Administration.

Administrators can configure additional roles for an application. A role contains, for a particular application, the list of resources that an application comprises. For each resource that a role comprises, the administrator defines the access privilege. For the Cisco Unified Communications Manager Administration application, the access privileges include read and update. Other applications specify their own access privileges.

Because Cisco Unified Communications Manager allows administrators to manage user groups, roles, and resources, no guarantee exists that a particular user group or role goes unchanged or that administrators will use the predefined user groups or roles.
Roles

The system groups the resources that are available to Cisco Unified Communications Manager Administration and to other applications into roles. A role includes a collection of resources for an application, such as Cisco Unified Communications Manager Administration. The following types of roles exist:

- **Custom roles**—Administrator-defined roles that you configure in Cisco Unified Communications Manager Administration after a Cisco Unified Communications Manager installation; for example, a help desk role.
- **Standard roles**—Default roles that get created automatically with Cisco Unified Communications Manager installation; you cannot modify or delete standard roles, but you can copy them to create custom roles, which allows you to modify them for your preferences. (See the table below for the list of standard roles and the privileges/resources that the role provides.)

Each role contains a group of resources, with privileges assigned to each resource. For most applications with graphical user interfaces, such as Cisco Unified Communications Manager Administration, privileges allow you to perform tasks, such as viewing or updating data, in a specific window or a group of related windows, which are defined as resources in the Role Configuration window. For example, for the Standard CCM Feature Management role, you can view and configure message waiting in the Message Waiting Configuration window in Cisco Unified Communications Manager Administration. For each role that is associated with Cisco Unified Communications Manager Administration, the specified privilege allows a certain level of access to each of the resources (windows). For example, privileges specify the following access in Cisco Unified Communications Manager Administration:

- **Read**—Allows users in a user group to view data in specific windows (defined as resources), but the user(s) cannot modify data in the window. Buttons such as Insert, Delete, Update, and Reset do not display.
- **Update**—Allows users in a user group to view and modify data in certain windows (defined as resources for the role). Users with the update privilege can perform operations such as Insert, Delete, Update, and Reset.

Other applications, such as CTI applications, specify their own access privileges and do not use the read and update privileges or a common list of resources (which are configuration windows in most cases); for example, the Standard CTI Allow Call Recording role allows CTI devices/CTI applications to record calls, and the Standard EM Authentication Proxy Rights manages Cisco Extension Mobility authentication rights for application users that interact with Cisco Extension Mobility.

---

**Note**

The Standard CCM Admin Users role gives the user access to the Cisco Unified Communications Manager Administration user interface. This role, the base role for all administration tasks, serves as the authentication role. Cisco Unified Communications Manager Administration defines this role as the role that is necessary to log in to Cisco Unified Communications Manager Administration.

The Standard CCM Admin Users role includes no permissions beyond logging into Cisco Unified Communications Manager Administration. The administrator must add another authorization role to define the parts of the Cisco Unified Communications Manager Administration that the user can administer. The Standard CCMADM IN Administration role allows a user to access and make changes in all of Cisco Unified Communications Manager Administration.
A user with only the Standard CCM Admin Users role can access Cisco Unified Communications Manager Administration but cannot make any changes. A user with only the Standard CCMADMIN Administration role can make changes, but cannot authenticate entry to Cisco Unified Communications Manager Administration.

A user, therefore, must have the Standard CCM Admin Users role to access Cisco Unified Communications Manager Administration and must have at least one other role to administer the system.

The following table lists the standard roles, the application(s) that the roles support, the privileges (resources) for the roles, and the standard user groups that are automatically associated with the standard roles.

For a role, supported privileges are checked in the Role Configuration window. For standard roles, you cannot change the configuration, but if you want to do so, you can copy a standard role to configure a custom role, which you can modify to your preferences.

### Table 1: Standard Roles and Privileges

<table>
<thead>
<tr>
<th>Standard Role</th>
<th>Supported Application(s)</th>
<th>Privileges/Resources for the Role</th>
<th>Associated Standard User Group(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard AXL API Access</td>
<td>AXL database API</td>
<td>Allows access to the AXL database API</td>
<td>Standard CCM Super Users</td>
</tr>
<tr>
<td>Standard Admin Rep Tool Admin</td>
<td>Cisco Unified Communications Manager CDR Analysis and Reporting (CAR)</td>
<td>Allows an administrator to view and configure Cisco Unified Communications Manager CDR Analysis and Reporting (CAR).</td>
<td>Standard CAR Admin Users, Standard CCM Super Users</td>
</tr>
<tr>
<td>Standard Audit Log Administration</td>
<td>Cisco Unified Serviceability</td>
<td>Allows an administrator to perform the following tasks for the audit logging feature:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• View and configure audit logging in the Audit Log Configuration window in Cisco Unified Serviceability</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• View and configure trace in Cisco Unified Serviceability and collect traces for the audit log feature in Real-Time Monitoring Tool</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• View and start/stop the Cisco Audit Event service in Cisco Unified Serviceability</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• View and update the associated alert in RTMT</td>
<td>Standard Audit Users</td>
</tr>
<tr>
<td>Standard Role</td>
<td>Supported Application(s)</td>
<td>Privileges/Resources for the Role</td>
<td>Associated Standard User Group(s)</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Standard CCM End Users</td>
<td>Cisco Unified CM User Options</td>
<td>Grant an end user log-in rights to the Cisco Unified CM User Options.</td>
<td>Standard CCM End Users</td>
</tr>
<tr>
<td>Standard CCM Feature Management</td>
<td>Cisco Unified Communications Manager Administration</td>
<td>Allows an administrator to perform the following tasks:</td>
<td>Standard CCM Server Maintenance</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• View, delete, and insert the following items by using the Bulk Administration Tool:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>◦ Client matter codes and forced authorization codes</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>◦ Call pickup groups</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• View and configure the following items in Cisco Unified Communications Manager Administration:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>◦ Client matter codes and forced authorization codes</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>◦ Call park</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>◦ Call pickup</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>◦ Meet-Me numbers/patterns</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>◦ Message Waiting</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>◦ Cisco Unified IP Phone Services</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>◦ Voice mail pilots, voice mail port wizard, voice mail ports, and voice mail profiles</td>
<td></td>
</tr>
<tr>
<td>Standard Role</td>
<td>Supported Application(s)</td>
<td>Privileges/Resources for the Role</td>
<td>Associated Standard User Group(s)</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>----------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Standard CCM Gateway Management</td>
<td>Cisco Unified Communications Manager Administration</td>
<td>Allows an administrator to perform the following tasks:</td>
<td>Standard CCM Gateway Administration</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• View and configure gateway templates in the Bulk Administration Tool</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• View and configure gatekeepers, gateways, and trunks in Cisco Unified Communications Manager Administration</td>
<td></td>
</tr>
<tr>
<td>Standard CCM Phone Management</td>
<td>Cisco Unified Communications Manager Administration</td>
<td>Allows an administrator to perform the following tasks:</td>
<td>Standard CCM Phone Administration</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• View and export phones in the Bulk Administration Tool</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• View and insert user device profiles in the Bulk Administration Tool</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• View and configure the following items in Cisco Unified Communications Manager Administration:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>◦ BLF speed dials</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>◦ CTI route points</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>◦ Default device profiles or default profiles</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>◦ Directory numbers and line appearances</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>◦ Firmware load information</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>◦ Phone button templates or softkey templates</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>◦ Phones</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>◦ Reorder phone button information for a particular phone by clicking the Modify Button Items button in the Phone Configuration window</td>
<td></td>
</tr>
<tr>
<td>Standard Role</td>
<td>Supported Application(s)</td>
<td>Privileges/Resources for the Role</td>
<td>Associated Standard User Group(s)</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-------------------------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------------------------------</td>
</tr>
</tbody>
</table>
| Standard CCM Route Plan Management| Cisco Unified Communications Manager Administration                                        | Allows an administrator to perform the following tasks in Cisco Unified Communications Manager Administration:  
  • View and configure application dial rules  
  • View and configure calling search spaces and partitions  
  • View and configure dial rules, including dial rule patterns  
  • View and configure hunt lists, hunt pilots, and line groups  
  • View and configure route filters, route groups, route hunt list, route lists, route patterns, and route plan report  
  • View and configure time period and time schedule  
  • View and configure translation patterns                                                                                           |                                  |
|                                  |                                                                                           |                                                                                                                                                                                                                                 |                                  |
| Standard CCM Service Management  | Cisco Unified Communications Manager Administration                                        | Allows an administrator to perform the following tasks:  
  • View and configure the following items in Cisco Unified Communications Manager Administration:  
    ◦ Annunciators, conference bridges, and transcoders  
    ◦ MOH audio sources and MOH servers  
    ◦ Media resource groups and media resource group lists  
    ◦ Media termination point  
    ◦ Cisco Unified Communications Manager Assistant wizard  
  • View and configure the Delete Managers, Delete Managers/Assistants, and Insert Managers/Assistants windows in the Bulk Administration Tool | Standard CCM Server Maintenance   |
<table>
<thead>
<tr>
<th>Standard Role</th>
<th>Supported Application(s)</th>
<th>Privileges/Resources for the Role</th>
<th>Associated Standard User Group(s)</th>
</tr>
</thead>
</table>
| Standard CCM System Management | Cisco Unified Communications Manager Administration | Allows an administrator to perform the following tasks:  
  • View and configure the following items in Cisco Unified Communications Manager Administration:  
    ◦ AAR groups  
    ◦ Cisco Unified Communications Managers (Cisco Unified CMs) and Cisco Unified Communications Manager groups  
    ◦ Date and time groups  
    ◦ Device defaults  
    ◦ Device pools  
    ◦ Enterprise parameters  
    ◦ Enterprise phone configuration  
    ◦ Locations  
    ◦ NTP servers  
    ◦ Plug-ins  
    ◦ Security profiles for phones that run SCCP or SIP; security profiles for SIP trunks  
    ◦ SRST references  
    ◦ Servers  
  • View and configure the Job Scheduler windows in the Bulk Administration Tool | Standard CCM Server Maintenance |
<p>| Standard CCM User Privilege Management | Cisco Unified Communications Manager Administration | Allows an administrator to view and configure application users in Cisco Unified Communications Manager Administration. |  |
| Standard CCMADMIN Administration | Cisco Unified Communications Manager Administration | Allows an administrator to view and configure all items in Cisco Unified Communications Manager Administration and the Bulk Administration Tool. | Standard CCM Super Users |
| Standard CCMADMIN Administration | Dialed Number Analyzer | Allows an administrator to view and configure information in Dialed Number Analyzer. |  |</p>
<table>
<thead>
<tr>
<th>Standard Role</th>
<th>Supported Application(s)</th>
<th>Privileges/Resources for the Role</th>
<th>Associated Standard User Group(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard CCMADMIN Read Only</td>
<td>Cisco Unified Communications Manager Administration</td>
<td>Allows an administrator to view configuration in Cisco Unified Communications Manager Administration and the Bulk Administration Tool.</td>
<td>Standard CCM Gateway Administration, Standard CCM Phone Administration, Standard CCM Read Only, Standard CCM Server Maintenance, Standard CCM Server Monitoring</td>
</tr>
<tr>
<td>Standard CCMADMIN Read Only</td>
<td>Dialed Number Analyzer</td>
<td>Allows an administrator to analyze routing configurations in Dialed Number Analyzer.</td>
<td></td>
</tr>
<tr>
<td>Standard CCMUSER Administration</td>
<td>Cisco Unified CM User Options</td>
<td>Allows access to the Cisco Unified CM User Options.</td>
<td>Standard CCM End Users</td>
</tr>
<tr>
<td>Standard CTI Allow Call Monitoring</td>
<td>Cisco Computer Telephone Interface (CTI)</td>
<td>Allows CTI applications/devices to monitor calls.</td>
<td>Standard CTI Allow Call Monitoring</td>
</tr>
<tr>
<td>Standard CTI Allow Call Park Monitoring</td>
<td>Cisco Computer Telephone Interface (CTI)</td>
<td>Allows CTI applications/devices to use call park.</td>
<td>Standard CTI Allow Call Park Monitoring</td>
</tr>
<tr>
<td>Standard CTI Allow Call Recording</td>
<td>Cisco Computer Telephone Interface (CTI)</td>
<td>Allows CTI applications/devices to record calls.</td>
<td>Standard CTI Allow Call Recording</td>
</tr>
<tr>
<td>Standard CTI Allow Calling Number Modification</td>
<td>Cisco Computer Telephone Interface (CTI)</td>
<td>Allows CTI applications to transform calling party numbers during a call</td>
<td>Standard CTI Allow Calling Number Modification</td>
</tr>
<tr>
<td>Standard CTI Allow Control of All Devices</td>
<td>Cisco Computer Telephone Interface (CTI)</td>
<td>Allows control of all CTI-controllable devices</td>
<td>Standard CTI Allow Control of All Devices</td>
</tr>
<tr>
<td>Standard CTI Allow Control of Phones supporting Connected Xfer and conf</td>
<td>Cisco Computer Telephone Interface (CTI)</td>
<td>Allows control of all CTI devices that supported connected transfer and conferencing</td>
<td>Standard CTI Allow Control of Phones supporting Connected Xfer and conf</td>
</tr>
<tr>
<td>Standard CTI Allow Control of Phones supporting Rollover Mode</td>
<td>Cisco Computer Telephone Interface (CTI)</td>
<td>Allows control of all CTI devices that supported rollover mode</td>
<td>Standard CTI Allow Control of Phones supporting Rollover Mode</td>
</tr>
<tr>
<td>Standard CTI Allow Reception of SRTP Key Material</td>
<td>Cisco Computer Telephone Interface (CTI)</td>
<td>Allows CTI applications to access and distribute SRTP key material</td>
<td>Standard CTI Allow Reception of SRTP Key Material</td>
</tr>
<tr>
<td>Standard Role</td>
<td>Supported Application(s)</td>
<td>Privileges/Resources for the Role</td>
<td>Associated Standard User Group(s)</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>--------------------------------------------------------</td>
<td>-----------------------------------------------------------------------</td>
<td>---------------------------------------------------------</td>
</tr>
<tr>
<td>Standard CTI Enabled</td>
<td>Cisco Computer Telephone Interface (CTI)</td>
<td>Enables CTI application control</td>
<td>Standard CTI Enabled</td>
</tr>
<tr>
<td>Standard CTI Secure Connection</td>
<td>Cisco Computer Telephone Interface (CTI)</td>
<td>Enables a secure CTI connection to Cisco Unified Communications Manager</td>
<td>Standard CTI Secure Connection</td>
</tr>
<tr>
<td>Standard CUReporting</td>
<td>Cisco Unified Reporting</td>
<td>Allows an administrator to view, download, generate, and upload reports in Cisco Unified Reporting.</td>
<td>Standard CCM Admin Users, Standard CCM Super Users</td>
</tr>
<tr>
<td>Standard EM Authentication Proxy Rights</td>
<td>Cisco Extension Mobility</td>
<td>Manages application Cisco Extension Mobility authentication rights; required for all application users that interact with Cisco Extension Mobility (for example, Cisco Unified Communications Manager Assistant, Cisco Web Dialer, and so on)</td>
<td>Standard CCM Super Users, Standard EM Authentication Proxy Rights</td>
</tr>
<tr>
<td>Standard Packet Sniffing</td>
<td>Cisco Unified Communications Manager Administration</td>
<td>Allows an administrator to access Cisco Unified Communications Manager Administration to enable packet sniffing (capturing)</td>
<td>Standard Packet Sniffer Users</td>
</tr>
<tr>
<td>Standard RealtimeAndTraceCollection</td>
<td>Cisco Unified Serviceability and Real-Time Monitoring Tool</td>
<td>Allows an administrator to view and use the SOAP Serviceability AXL APIs, the SOAP Call Record APIs, the SOAP Diagnostic Portal (Analysis Manager) Database Service; view and configure trace for the audit log feature, and view and configure the Real-Time Monitoring Tool, including collecting traces in RTMT.</td>
<td>Standard RealtimeAndTraceCollection</td>
</tr>
<tr>
<td>Standard Role</td>
<td>Supported Application(s)</td>
<td>Privileges/Resources for the Role</td>
<td>Associated Standard User Group(s)</td>
</tr>
<tr>
<td>---------------</td>
<td>--------------------------</td>
<td>-----------------------------------</td>
<td>-----------------------------------</td>
</tr>
</tbody>
</table>
| Standard SERVICEABILITY | Cisco Unified Serviceability and Real-Time Monitoring Tool | Allows an administrator to view and configure the following windows in Cisco Unified Serviceability or the Real-Time Monitoring Tool:  
  - Alarm Configuration and Alarm Definitions (Cisco Unified Serviceability)  
  - Audit Trace (marked as read/view only)  
  - SNMP-related windows (Cisco Unified Serviceability)  
  - Trace Configuration and Troubleshooting Trace Configuration (Cisco Unified Serviceability)  
  - Log Partition Monitoring  
  - Alert Configuration (RTMT), Profile Configuration (RTMT), Trace Collection (RTMT)  

Allows an administrator to view and use the SOAP Serviceability AXL APIs, the SOAP Call Record APIs, and the SOAP Diagnostic Portal (Analysis Manager) Database Service.  
**Tip** For the SOAP Call Record API, the RTMT Analysis Manager Call Record permission is controlled through this resource.  
**Tip** For the SOAP Diagnostic Portal Database Service, the RTMT Analysis Manager Hosting Database access controlled thorough this resource. | Standard CCM Server Monitoring, Standard CCM Super Users |
| Standard SERVICEABILITY Administration | Cisco Unified Communications Manager Administration | A serviceability administrator can access the Plugin window in Cisco Unified Communications Manager Administration and download plugins from this window. | |
| Standard SERVICEABILITY Administration | Dialed Number Analyzer | Allows an administrator to administer all aspects of serviceability for Dialed Number Analyzer. | |
| Standard SERVICEABILITY Administration | Cisco Unified Serviceability and Real-Time Monitoring Tool | Allows an administrator to view and configure all windows in Cisco Unified Serviceability and RTMT. (Audit Trace supports viewing only.) Allows an administrator to view and use all SOAP Serviceability AXL APIs. | |
## User groups

After configuration of custom roles, you can configure user groups, which are a collection of Cisco Unified Communications Manager application users and end users that get grouped together for the purpose of assigning a common list of roles to the members in the user group. Like standard roles, standard user groups get created at installation, and you cannot delete these user groups; you can only add or delete application or end users from standard user groups.

Standard user groups in Cisco Unified Communications Manager Administration provide a predefined set of roles and permissions for various functions. Administrators can manage user groups, roles, and permissions to control the level of access (and, therefore, the level of security) for system users.

Various named user groups that are predefined have no members that are assigned to them at install time. The Cisco Unified Communications Manager super user or a user with access to user group configuration should add users to these groups. The super user or a user with access to user group configuration can configure additional named user groups as needed.

<table>
<thead>
<tr>
<th>Standard Role</th>
<th>Supported Application(s)</th>
<th>Privileges/Resources for the Role</th>
<th>Associated Standard User Group(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard SERVICEABILITY Read Only</td>
<td>Dialed Number Analyzer</td>
<td>Allows an administrator to view all serviceability-related data for components in Dialed Number Analyzer.</td>
<td>Standard CCM Read Only</td>
</tr>
<tr>
<td>Standard SERVICEABILITY Read Only</td>
<td>Cisco Unified Serviceability and Real-Time Monitoring Tool</td>
<td>Allows an administrator to view configuration in Cisco Unified Serviceability and RTMT. (excluding audit configuration window, which is represented by the Standard Audit Log Administration role) Allows an administrator to view all SOAP Serviceability AXL APIs, the SOAP Call Record APIs, and the SOAP Diagnostic Portal (Analysis Manager) Database Service.</td>
<td></td>
</tr>
<tr>
<td>Standard System Service Management</td>
<td>Cisco Unified Serviceability</td>
<td>Allows an administrator to view, activate, start, and stop services in Cisco Unified Serviceability.</td>
<td></td>
</tr>
</tbody>
</table>

---

**Note**

The Standard CCM Super Users user group represents a named user group that always has full access permission to all named roles. You cannot delete this user group. You can only make additions and deletions of users to this group.

---

**Note**

CCMA administrator always represents a super user.

Certain user groups and roles exhibit limitations that administrators need to recognize. For example, you can modify the Standard EM Authentication Proxy Rights user group by adding both application users and end
users. Because authentication by proxy is intended for use by applications, end users that get added to this user group cannot authenticate by proxy.

**Access log**

The log contains a file report of access/change attempts. That is, Cisco Unified Communications Manager Administration generates a record of attempts to access or modify any directory or database component through Cisco Unified Communications Manager Administration. The change record includes the user name, date, time, window from which the change was made, and the success or failure status of the update.

**Enterprise parameters**

Roles and user groups use the Effective Access Privileges For Overlapping User Groups and Roles enterprise parameter.

**Effective Access Privileges for Overlapping User Groups and Roles**

The Effective Access Privileges For Overlapping User Groups and Roles enterprise parameter determines the level of user access for users that belong to multiple user groups and have conflicting privileges.

You can set this enterprise parameter to the following values:

- Maximum-The effective privilege represents the maximum of the privileges of all the overlapping user groups.
- Minimum-The effective privilege represents the minimum of the privileges of all the overlapping user groups.

The Effective Access Privileges For Overlapping User Groups and Roles enterprise parameter specifies the maximum default value.

---

**Note**

This enterprise parameter does not affect the privileges for the members of the Standard CCM Super Users user group.

---

**Create a custom help desk role and user group**

Some companies want their help desk personnel to have privileges to be able to perform certain tasks, such as adding a phone, adding an end user, or adding an end user to a user group in Cisco Unified Communications Manager Administration.

Performing the steps in the following example allows help desk personnel to add a phone, add an end user, and add the end user to the Standard CCM End Users user group, which allows an end user to access and update the Cisco Unified CM User Options.

**Example-Allows Help Desk Personnel to Add Phone, Add End User, and Add End User to User Group**
Procedure

Step 1 In Cisco Unified Communications Manager Administration, choose **User Management > Role**.

Step 2 Click **Add New**.

Step 3 From the Application drop-down list box, choose **Cisco Call Manager Administration**; then, click **Next**.

Step 4 In the Name field, enter the name of the role; for example, Help Desk.

Step 5 In the Description field, enter a short description; for example, for adding phones and users.

Step 6 Choose one of the following options, which depends on where you want the help desk personnel to perform the task:

   a) If you want the help desk personnel to add a phone in the Phone Configuration window and then add an end user in the End User Configuration window, check the read and update privileges check boxes for the User web page resource and the Phone web pages resource; then, click **Save**.

   b) If you want the help desk personnel to add both a phone and user at the same time in the User and Phone Add window, check the read and update privileges check boxes for the User and Phone add resource and the User web page resource; then click **Save**.

Step 7 By performing the following tasks, create a custom user group for the help desk:

   a) In Cisco Unified Communications Manager Administration, choose **User Management > User Group**; then, click **Add New**.

   b) Enter the name of the custom user group; for example, Help Desk.

   c) From the Related Links drop-down list box, choose **Assign Roles to User Group**; then, click **Go**.

   d) Click the **Assign Role to Group** button.

   e) Check the check box for the custom role that you created in Step 6; in this example, Help Desk. In addition, check the check box for the Standard CCM Admin Users role. Then, click **Add Selected**.

   f) In the User Group Configuration window, verify that the roles display in the Role Assignment pane; then, click **Save**.

What to Do Next

In Cisco Unified Communications Manager Administration, the help desk personnel can add the phone, add the user, and add the end user to the user group.

   • To add a phone in the Phone Configuration window, choose **Device > Phone**; then, to add an end user in the End User Configuration window, choose **User Management > End User**.

   • To add both a phone and user at the same time in the User and Phone Add window, choose **User Management > User and Phone Add**.

   • To associate the end user with the Standard CCM End Users user group, choose **User Management > User Group**.
Create a custom help desk role and user group
System-level configuration settings

This chapter provides information about configuring system-level settings before you add devices and configure other Cisco Unified Communications Manager features.

- System configuration, page 29
- Server configuration, page 30
- Hostname configuration, page 31
- Cisco Unified Communications Manager configuration, page 33
- Cisco Unified Communications Manager groups, page 33
- NTP reference configuration, page 35
- Date/time groups, page 35
- Locations and regions, page 36
- Device pools, page 45
- Common device configuration, page 47
- LDAP, page 48
- Call Admission Control, page 48
- Survivable Remote Site Telephony references, page 49
- MLPP domain, page 50
- Enterprise parameters, page 51
- Service parameters, page 51
- Dependency records, page 51

System configuration

Before you add devices and configure Cisco Unified Communications Manager features, configure system-level settings, such as servers, regions, device pools, and so on.
Procedure

**Step 1** Configure the server to specify the address of the server where Cisco Unified Communications Manager is installed.

**Step 2** Specify the ports and other properties for Cisco Unified Communications Manager.

**Step 3** Configure phone NTP references, so phones that are running SIP can get the date and time from the NTP server (optional).

**Step 4** Configure Date/Time groups to define time zones for the various devices that are connected to Cisco Unified Communications Manager.

**Step 5** Configure regions to specify the maximum bit rate that can be used for calls between devices within that region, and between that region and other regions, if needed.

  **Tip** You do not need to configure regions if you are using only the default G.711 audio codec.

**Step 6** Configure device pools to define a set of common characteristics that can be assigned to devices.

**Step 7** Configure media resource groups and media resource group lists.

**Step 8** Configure LDAP to store authentication and authorization information about users who interface with Cisco Unified Communications Manager.

**Step 9** Configure locations or gatekeepers for call admission control.

**Step 10** Configure survivable remote site telephony (SRST) references to preserve rudimentary call capability.

**Step 11** Configure the MLPP domain.

**Step 12** Update enterprise parameters, if necessary.

**Step 13** Update service parameters, if necessary. For example, configure the DRF backup and restore master agent in the Cisco Unified Communications Manager Administration Service Parameters Configuration window.

**Related Topics**

Server configuration, on page 30
Cisco Unified Communications Manager configuration, on page 33
NTP reference configuration, on page 35
Date/time groups, on page 35
Regions, on page 37
Device pools, on page 45
Survivable Remote Site Telephony references, on page 49
MLPP domain, on page 50
Enterprise parameters, on page 51
Service parameters, on page 51
Dependency records, on page 51
Media resource management, on page 245

**Server configuration**

Use the server configuration to specify the address of the server where Cisco Unified Communications Manager is installed. If your network uses Domain Name System (DNS) services, you can specify the host name of
the server. If your network does not use DNS services, you must specify the Internet Protocol Version 4 (IPv4) address of the server.

**Configuring a Server**

The following guidelines apply to configuring (adding and updating) a server:

- If your network supports IPv4, you must update the DNS server with the appropriate Cisco Unified Communications Manager name and address information before using that information to configure the Cisco Unified Communications Manager server.

- Cisco Unified Communications Manager Administration does not prevent you from updating the IP Address field under any circumstances.

- When you attempt to change the IP address in the Server Configuration window, the following message displays after you save the configuration: “Changing the host name/IP Address of the server may cause problems with Cisco Unified Communications Manager. Are you sure that you want to continue?” Before you click OK, make sure that you understand the implications of updating the Host Name/IP Address field; for example, updating this setting incorrectly may cause Cisco Unified Communications Manager to become inoperable; that is, the database may not work, you may not be able to access Cisco Unified Communications Manager Administration, and so on. In addition, updating this field without performing other related tasks may cause problems for Cisco Unified Communications Manager.

- For additional information on changing the IP address or host name, see the document, Changing the IP Address and Host Name for Cisco Unified Communications Manager Release 8.5(1).

- Any changes that you make to the server configuration do not take effect until you restart Cisco Unified Communications Manager.

**Deleting a Server**

You cannot delete the server where you installed Cisco Unified Communications Manager Business Edition 5000.

**Related Topics**

- System configuration, on page 29
- Security enabled for annunciator, on page 259

**Hostname configuration**

The following table lists the locations where you can configure a host name for the Cisco Unified Communications Manager server, the allowed number of characters for the host name, and the recommended first and last characters for the host name. Be aware that, if you do not configure the host name correctly, some components in Cisco Unified Communications Manager, such as the operating system, database, installation, and so on, may not work as expected.
Before you change the host name or IP address for any locations that are listed in the following table, see Changing the IP Address and Host Name for Cisco Unified Communications Manager 8.5(1). Failing to update the host name or IP address correctly after it is configured may cause problems for Cisco Unified Communications Manager.

### Table 2: Host Name Configuration in Cisco Unified Communications Manager

<table>
<thead>
<tr>
<th>Host Name Location</th>
<th>Allowed Configuration</th>
<th>Allowed Number of Characters</th>
<th>Recommended First Character for Host Name</th>
<th>Recommended Last Character for Host Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Name/ IP Address field</td>
<td>You can add or change the host name for a server in the cluster.</td>
<td>2-63</td>
<td>alphabetic</td>
<td>alphanumeric</td>
</tr>
<tr>
<td>System &gt; Server in Cisco Unified Communications Manager Administration</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hostname field</td>
<td>You can add the host name for a server in the cluster.</td>
<td>1-63</td>
<td>alphabetic</td>
<td>alphanumeric</td>
</tr>
<tr>
<td>Cisco Unified Communications Manager installation</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hostname field</td>
<td>You can change, not add, the host name for a server in the cluster.</td>
<td>1-63</td>
<td>alphabetic</td>
<td>alphanumeric</td>
</tr>
<tr>
<td>Settings &gt; IP &gt; Ethernet in Cisco Unified Communications Operating System</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>set network hostname</td>
<td>You can change, not add, the host name for a server in the cluster.</td>
<td>1-63</td>
<td>alphabetic</td>
<td>alphanumeric</td>
</tr>
<tr>
<td>hostname Command Line Interface</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Caution:**

The host name must follow the rules for ARPANET host names. Between the first and last character of the host name, you can enter alphanumeric characters and hyphens.

Before you configure the host name in any location in Table 5-2, review the following information:

- The Host Name/IP Address field in the Server Configuration window, which supports device-to-server, application-to-server, and server-to-server communication, allows you to enter an IPv4 address in dotted decimal format or a host name.
- After you install Cisco Unified Communications Manager on the publisher database server, the host name for the publisher automatically displays in this field. Before you install Cisco Unified Communications Manager on the subscriber server, enter either the IP address or the host name for the subscriber server in this field on the publisher database server.
In this field, only configure a hostname if Cisco Unified Communications Manager can access the DNS server to resolve host names to IP addresses; make sure that you configure the Cisco Unified Communications Manager name and address information on the DNS server.

**Tip**

In addition to configuring Cisco Unified Communications Manager information on the DNS server, you enter DNS information during the Cisco Unified Communications Manager installation.

- During the Cisco Unified Communications Manager installation of the publisher database server, you enter the host name, which is mandatory, and IP address of the publisher server to configure network information; that is, if you want to use static networking. During the Cisco Unified Communications Manager installation on the subscriber server, you enter the hostname and IP address of the publisher database server, so Cisco Unified Communications Manager can verify network connectivity and publisher-subscriber validation. Additionally, you must enter the host name and the IP address for the subscriber server. When the Cisco Unified Communications Manager installation prompts you for the host name of the subscriber server, enter the value that displays in the Server Configuration window in Cisco Unified Communications Manager Administration; that is, if you configured a host name for the subscriber server in the Host Name/IP Address field.

### Cisco Unified Communications Manager configuration

The Cisco Unified Communications Manager servers get added to Cisco Unified Communications Manager at installation time. Use Cisco Unified Communications Manager configuration to update fields such as the ports and other properties for each Cisco Unified Communications Manager that is installed.

Any changes that you make to the settings for auto-registration partition, external phone number mask, and voice message box mask do not take effect until you restart Cisco Unified Communications Manager.

**Note**

When you perform a fresh installation of Cisco Unified Communications Manager, you must activate the Cisco CallManager service. For information about activating the Cisco CallManager service, see the Cisco Unified Serviceability Administration Guide.

**Related Topics**

System configuration, on page 29

### Cisco Unified Communications Manager groups

A Cisco Unified Communications Manager group comprises a prioritized list of up to three Cisco Unified Communications Managers. The first Cisco Unified Communications Manager in the list serves as the primary Cisco Unified Communications Manager for that group, and the other members of the group serve as secondary (backup) Cisco Unified Communications Managers.

Cisco Unified Communications Manager groups associate with devices through device pools. Each device belongs to a device pool, and each device pool specifies the Cisco Unified Communications Manager group for all of its devices.
Some Media Gateway Control Protocol (MGCP) devices, such as gateways and route/hunt lists, can associate directly with Cisco Unified Communications Manager groups.

Cisco Unified Communications Manager groups provide two important features for your system:

- Prioritized failover list for backup call processing—When a device registers, it attempts to connect to the primary (first) Cisco Unified Communications Manager in the group that is assigned to its device pool. If the primary Cisco Unified Communications Manager is not available, the device tries to connect to the next Cisco Unified Communications Manager that is listed in the group, and so on. Each device pool has one Cisco Unified Communications Manager group that is assigned to it.

- Call processing load balancing—You can configure device pools and Cisco Unified Communications Manager groups to distribute the control of devices across multiple Cisco Unified Communications Managers. See the Balanced call processing, on page 56 for more information.

For most systems, you will assign a single Cisco Unified Communications Manager to multiple groups to achieve better load distribution and redundancy.

**Adding a Cisco Unified Communications Manager Group**

- Cisco Unified Communications Managers automatically get installed and configured.

- Each Cisco Unified Communications Manager cluster can have only one default auto-registration group. If you choose a different Cisco Unified Communications Manager group as the default auto-registration group, the previously chosen auto-registration group no longer serves as the default for the cluster.

- You must reset the devices that use the updated Cisco Unified Communications Manager group to apply any changes that you make.

**Deleting a Cisco Unified Communications Manager Group**

You cannot delete a Cisco Unified Communications Manager group if it is assigned to any device pools or MGCP gateways or if it is the current Auto-registration Cisco Unified Communications Manager Group for the cluster.

To find out which devices are using the Cisco Unified Communications Manager group, choose Dependency Records from the Related Links drop-down list box on the Cisco Unified Communications Manager Group Configuration window and click Go.

Before deleting a Cisco Unified Communications Manager group that is currently in use, you must perform some or all of the following tasks:

- Assign a different Cisco Unified Communications Manager group to the device pools or MGCP gateways that currently use this Cisco Unified Communications Manager group.

- Create or choose a different Cisco Unified Communications Manager group to be the Auto-registration Cisco Unified Communications Manager Group.

For more information, see the Cisco Unified Communications Manager Administration Guide and the Cisco Cisco Unified Serviceability Administration Guide.
NTP reference configuration

You can configure phone Network Time Protocol (NTP) references in Cisco Unified Communications Manager Administration to ensure that an IP phone that is running SIP gets its date and time from an NTP server. If a phone that is running SIP cannot get its date/time from the provisioned “Phone NTP Reference,” the phone will receive this information when it registers with Cisco Unified Communications Manager.

Adding a Phone NTP Reference

After you add the phone NTP reference to Cisco Unified Communications Manager Administration, you must add it to a date/time group. In the date/time group, you prioritize the phone NTP references, starting with the first server that you want the phone to contact.

The date/time group configuration gets specified in the device pool, and the device pool gets specified on the phone window.

Deleting a Phone NTP Reference

Before you can delete a phone NTP reference from Cisco Unified Communications Manager Administration, you must delete the server from the date/time group. To find which date/time groups use the phone NTP reference, choose Dependency Records from the Related Links drop-down list box in the Phone NTP Reference Configuration window and click Go.

If the dependency records feature is not enabled for the system, the dependency records summary window displays a message that shows the action that you can take to enable the dependency records; the message also displays information about high CPU consumption that is related to the dependency records feature.

Related Topics

- Balanced call processing, on page 56
- System configuration, on page 29

Date/time groups

Use Date/Time Groups to define time zones for the various devices that are connected to Cisco Unified Communications Manager.

Cisco Unified Communications Manager provides a default Date/Time Group that is called CMLocal that configures automatically when you install Cisco Unified Communications Manager; however, Cisco recommends that you configure a group for each local time zone. CMLocal synchronizes to the active date and time of the operating system on the Cisco Unified Communications Manager server. After installing Cisco Unified Communications Manager, you can change the settings for CMLocal as desired. Normally, you adjust the server date/time to the local time zone date and time.

Note

CMLocal resets to the operating system date and time whenever you restart Cisco Unified Communications Manager or upgrade the Cisco Unified Communications Manager software to a new release. Do not change the name of CMLocal.
For a worldwide distribution of Cisco Unified IP Phones, create a Date/Time Group for each of the 24 time zones.

Tip
To ensure that Cisco Unified Communications Manager includes the latest time zone information, you can install a COP file that updates the time zone information after you install Cisco Unified Communications Manager. You do not need to upgrade Cisco Unified Communications Manager to get these updates. After major time zone change events, Cisco contacts you to let you know that you can download COP file ciscocm.dst-updater.YYYYv-1.el4.x.y.z.cop to install on the servers in your cluster. (In the preceding file name example, “YYYY” represents the release year of the COP file, “v” specifies the file version number, and “x.y.z ”specifies the Cisco Unified Communications Manager.).

Be aware that COP files that contain “x.y.z” in their filenames are compatible with only Release x.y(z).

For information about how to install a COP file, follow the installation instructions that you get with the file.

Adding a Date/Time Group

After adding a new date/time group to the database, you can assign it to a device pool to configure the date and time information for that device pool.

You must reset devices to apply any changes that you make.

Deleting a Date/Time Group

You cannot delete a date/time group that any device pool uses.

To find out which device pools use the Date/Time Group, choose Dependency Records from the Related Links drop-down list box on the Date/Time Group Configuration window and click Go.

Before deleting a Date/Time Group that is currently in use, you must perform either or both of the following tasks:

- Assign a different Date/Time Group to device pools that use the Date/Time Group that you want to delete.
- Delete the device pools that use the Date/Time Group that you want to delete.

Related Topics

- Device pools, on page 45
- System configuration, on page 29

Locations and regions

You must assign each device on the network to both a region (by means of a device pool) and a location.
In Cisco Unified Communications Manager, locations-based call admission control works in conjunction with regions to define the characteristics of a network link:

- Regions define the maximum bit rate, and hence, the type of codec, that is used on the link (and therefore, the amount of bandwidth that is used per call).
- Locations define the amount of available bandwidth for the link.

**Related Topics**

[Call Admission Control, on page 48](#)

**Regions**

Regions provide capacity controls for Cisco Unified Communications Manager multi-site deployments where you may need to limit the bandwidth for individual calls that are sent across a WAN link, but where you want to use a higher bandwidth for internal calls. Additionally, the system uses regions also for applications that only support a specific codec; for example, an application that only uses G.711. Use regions to specify the maximum transport-independent bit rate that is used for audio and video calls within a region and between regions; in this case, codecs with higher bit rates do not get used for the call.

Cisco Unified Communications Manager prefers codecs with better audio quality. For example, despite having a maximum bit rate of 32 kb/s, G.722.1 sounds better than some codecs with higher bit rates, such as G.711, which has a bit rate of 64 kb/s.

When you configure the maximum audio bit rate setting in the Region Configuration window (or use the service parameter in the Service Parameter Configuration window), this setting serves as a filter. When an audio codec is selected for a call, Cisco Unified Communications Manager takes the matching codecs from both sides of a call leg, filters out the codecs that exceed the configured maximum audio bit rate, and then picks the preferred codec among the codecs that are remaining in the list.

The audio codec preference feature orders the audio preference in the following table for the default low-loss case by sound quality, and the table adds a separate preference list for the lossy case.

**Table 3: Audio Codec Preference Order for Cisco Unified Communications Manager 8.6(1)**

<table>
<thead>
<tr>
<th>If Low Loss Is Configured for Link Loss Type</th>
<th>If Lossy Is Configured for Link Loss Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>AMR-WB-24 kb/s</td>
<td>AMR-WB-24 kb/s</td>
</tr>
<tr>
<td>AMR-13 kb/s</td>
<td>AMR-13 kb/s</td>
</tr>
<tr>
<td>AAC-LD (MP4A-LATM)-128 kb/s</td>
<td>AAC-LD (MP4A-LATM)-128 kb/s</td>
</tr>
<tr>
<td>AAC-LD (mpeg4-generic)-64 kb/s</td>
<td>AAC-LD (mpeg4-generic)-64 kb/s</td>
</tr>
<tr>
<td>AAC-LD (MP4A-LATM)-64 kb/s</td>
<td>AAC-LD (MP4A-LATM)-64 kb/s</td>
</tr>
<tr>
<td>AAC-LD (MP4A-LATM)-56 kb/s</td>
<td>AAC-LD (MP4A-LATM)-56 kb/s</td>
</tr>
<tr>
<td>L16-256 kb/s</td>
<td>L16-256 kb/s</td>
</tr>
<tr>
<td>AAC-LD (MP4A-LATM)-48 kb/s</td>
<td>AAC-LD (MP4A-LATM)-48 kb/s</td>
</tr>
<tr>
<td>If Low Loss Is Configured for Link Loss Type</td>
<td>If Lossy Is Configured for Link Loss Type</td>
</tr>
<tr>
<td>-----------------------------------------</td>
<td>-----------------------------------------</td>
</tr>
<tr>
<td>G.722 64k-64 kb/s</td>
<td>iSAC-32 kb/s</td>
</tr>
<tr>
<td>iSAC-32 kb/s</td>
<td>AAC-LD (MP4A-LATM)-32 kb/s</td>
</tr>
<tr>
<td>AAC-LD (MP4A-LATM)-32 kb/s</td>
<td>G.722 64k-64 kb/s</td>
</tr>
<tr>
<td>G.722.1 32k-32 kb/s</td>
<td>G.722.1 32k-32 kb/s</td>
</tr>
<tr>
<td>G.722 -56 kb/s</td>
<td>G.722 -56 kb/s</td>
</tr>
<tr>
<td>G.722-48 kb/s</td>
<td>G.722-48 kb/s</td>
</tr>
<tr>
<td>AAC-LD (MP4A-LATM)-24 kb/s</td>
<td>AAC-LD (MP4A-LATM)-24 kb/s</td>
</tr>
<tr>
<td>G.711 mu-law 64 k-64 kb/s</td>
<td>G.711 mu-law 64 k-64 kb/s</td>
</tr>
<tr>
<td>G.711 A-law 64k-64 kb/s</td>
<td>G.711 A-law 64k-64 kb/s</td>
</tr>
<tr>
<td>G.711 mu-law 56k-56 kb/s</td>
<td>G.711 mu-law 56k-56 kb/s</td>
</tr>
<tr>
<td>G.711 A-law 56k-56kb/s</td>
<td>G.711 A-law 56k-56kb/s</td>
</tr>
<tr>
<td>iLBC-16 kb/s</td>
<td>iLBC-16 kb/s</td>
</tr>
<tr>
<td>G.728-16 kb/s</td>
<td>G.728-16 kb/s</td>
</tr>
<tr>
<td>GSM Enhanced Full Rate-13 kb/s</td>
<td>GSM Enhanced Full Rate-13 kb/s</td>
</tr>
<tr>
<td>GSM Full Rate-13 kb/s</td>
<td>GSM Full Rate-13 kb/s</td>
</tr>
<tr>
<td>G.729b-8 kb/s</td>
<td>G.729b-8 kb/s</td>
</tr>
<tr>
<td>G.729ab-8 kb/s</td>
<td>G.729ab-8 kb/s</td>
</tr>
<tr>
<td>G.729-8 kb/s</td>
<td>G.729-8 kb/s</td>
</tr>
<tr>
<td>G.729a-8 kb/s</td>
<td>G.729a-8 kb/s</td>
</tr>
<tr>
<td>GSM Half Rate-7 kb/s</td>
<td>GSM Half Rate-7 kb/s</td>
</tr>
<tr>
<td>G.723.1-7 kb/s</td>
<td>G.723.1-7 kb/s</td>
</tr>
</tbody>
</table>

For calls made between Cisco Unified Communications Manager and previous versions of Cisco Unified Communications Manager over SIP intercluster trunks, the Cisco Unified Communications Manager that makes the SDP Answer chooses the codec. Because of SIP Delayed Offer support, the Cisco Unified
Communications Manager that initiates or resumes the call is the one that makes the SDP Answer, and hence, it is the one that determines the codec for the call.

For audio calls that involve H.323 intercluster trunks, Cisco Unified Communications Manager uses the preference list of codecs in the previous table only if both sides of the call run Cisco Unified Communications Manager 8.6(1). If both sides of the call do not run Cisco Unified Communications Manager 8.6(1), the codec list from the following table gets used.

For audio and video calls, Cisco Unified Communications Manager uses the preference order of codecs in the following table.

*Table 4: Audio Codec Preference Order for H.323 Intercluster Trunks If Both Sides of Call Do Not Support Cisco Unified Communications Manager 8.5(1)*

<table>
<thead>
<tr>
<th>If Lossy Is Configured for Link Loss Type</th>
<th>If Low Lossy Is Configured for Link Loss Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>---</td>
<td>iLBC-16 kb/s</td>
</tr>
<tr>
<td>AAC-LD (mpeg4-generic)-256 kb/s</td>
<td>AAC-LD (mpeg4-generic)-256 kb/s</td>
</tr>
<tr>
<td>L16-256 kb/s</td>
<td>L16-256 kb/s</td>
</tr>
<tr>
<td>G.722.1 24k-24 kb/s</td>
<td>G.722.1 24k-24 kb/s</td>
</tr>
<tr>
<td>G.722.1 32k-32 kb/s</td>
<td>G.722.1 32k-32 kb/s</td>
</tr>
<tr>
<td>G.722 64k-64 kb/s</td>
<td>G.722 64k-64 kb/s</td>
</tr>
<tr>
<td>G.711 mu-law 64k-64 kb/s</td>
<td>G.711 mu-law 64k-64 kb/s</td>
</tr>
<tr>
<td>G.711 A-law 64k-64 kb/s</td>
<td>G.711 A-law 64k-64 kb/s</td>
</tr>
<tr>
<td>G.722 56k-56 kb/s</td>
<td>G.722 56k-56 kb/s</td>
</tr>
<tr>
<td>G.711 mu-law 56k-56 kb/s</td>
<td>G.711 mu-law 56k-56 kb/s</td>
</tr>
<tr>
<td>G.711 A-law 56k-56 kb/s</td>
<td>G.711 A-law 56k-56 kb/s</td>
</tr>
<tr>
<td>G.722 48k-48 kb/s</td>
<td>G.722 48k-48 kb/s</td>
</tr>
<tr>
<td>iLBC-16 kb/s</td>
<td>---</td>
</tr>
<tr>
<td>G.728-16 kb/s</td>
<td>G.728-16 kb/s</td>
</tr>
<tr>
<td>GSM Enhanced Full Rate-13 kb/s</td>
<td>GSM Enhanced Full Rate-13 kb/s</td>
</tr>
<tr>
<td>GSM Full Rate-13 kb/s</td>
<td>GSM Full Rate-13 kb/s</td>
</tr>
<tr>
<td>G.729b-8 kb/s</td>
<td>G.729b-8 kb/s</td>
</tr>
<tr>
<td>G.729ab-8kb/s</td>
<td>G.729ab-8kb/s</td>
</tr>
</tbody>
</table>
### Supported Audio Codecs

Cisco Unified Communications Manager supports video stream encryption and various audio/video codecs, such as G.722. Cisco Unified Communications Manager supports the following audio codecs:

- **G.711** - The most commonly supported codec, used over the public switched telephone network.
- **G.722** - G.722 is wideband codec that is always preferred by Cisco Unified Communications Manager over G.711, unless G.722 is disabled. Audio codec often used in video conferences. See the Codec usage, on page 501 of the Cisco Unified IP phones, on page 459 chapter for a detailed discussion of the Advertise G.722 Codec enterprise parameter, which determines whether Cisco Unified IP Phones will advertise the G.722 codec to Cisco Unified Communications Manager.
- **G.722.1** - G.722.1 is a low-complexity wideband codec operating at 24 and 32 kb/s. The audio quality approaches that of G.722 while using at most half the bit rate. As it is optimized for both speech and music, G.722.1 has slightly lower speech quality than the speech-optimized iSAC codec. G.722.1 is supported for SIP and H.323 devices.
- **G.723.1** - Low-bit-rate codec with 6.3 or 5.3 kb/s compression for Cisco IP Phone 12 SP+ and Cisco IP Phone 30 VIP devices.
- **G.728** - Low-bit-rate codec that video endpoints support.
- **G.729** - Low-bit-rate codec with 8-kb/s compression that is supported by Cisco Unified IP Phone 7900. Typically, you would use low-bit-rate codecs for calls across a WAN link because they use less bandwidth. For example, the factory default intraregion maximum audio bit rate is 64 kbps, while the factory default interregion maximum audio bit rate is 8 kbps.
- **GSM** - The global system for mobile communications (GSM) codec. GSM enables the MNET system for GSM wireless handsets to operate with Cisco Unified Communications Manager. Assign GSM devices to a device pool that specifies 13 kb/s as the audio codec for calls within the GSM region and between other regions. Depending on device capabilities, this includes GSM EFR (enhanced full rate) and GSM FR (full rate).
- **L16** - Uncompressed 16-bit linear pulse-code modulation (PCM) encoded audio with a 16-kHz sampling rate provides wideband audio at 256 kb/s. Works with phones with handsets, acoustics, speakers, and microphones that can support high-quality audio bandwidth, such as the Cisco Unified IP Phone 7900 Series.
- **AAC-LD (mpeg4-generic)** - Advanced Audio Coding-Low Delay (AAC-LD) is a super-wideband audio codec that provides superior sound quality for voice and music. This codec provides equal or improved sound quality over older codecs, even at lower bit rates.

AAC-LD (mpeg4-generic) is supported for SIP devices, in particular, Cisco TelePresence systems.
• AAC-LD (MP4A-LATM)-Advanced Audio Coding-Low Delay (AAC-LD) Low-overhead MPEG-4 Audio Transport Multiplex (LATM) is a super-wideband audio codec that provides superior sound quality for voice and music. This codec provides equal or improved sound quality over older codecs, even at lower bit rates.

AAC-LD (MP4A-LATM) is supported for SIP devices including Tandberg and some third-party endpoints.

**Note**
AAC-LD (mpeg4-generic) and AAC-LD (MPA4-LATM) are not compatible.

• iSAC-Internet Speech Audio Codec (iSAC) is an adaptive wideband audio codec, specially designed to deliver wideband sound quality with low delay in both low and medium-bit rate applications.

Using an adaptive bit rate of between 10 and 32 kb/s, iSAC provides audio quality approaching that of G.722 while using less than half the bandwidth. In deployments with significant packet loss, delay, or jitter, such as over a WAN, iSAC audio quality is superior to that of G.722 due to its robustness.

iSAC is supported for SIP and SCCP devices. The Cisco Unified Communications Manager IP Voice Media Streaming App (IPVMSApp), which includes Media Termination Point, Conference Bridge, Music on Hold Server, and Annunciator does not support iSAC. MGCP devices are not supported.

• iLBC-Internet Low Bit Rate Codec (iLBC) provides audio quality between that of G.711 and G.729 at bit rates of 15.2 and 13.3 kb/s, while allowing for graceful speech quality degradation in a lossy network due to the speech frames being encoded independently. By comparison, G.729 does not handle packet loss, delay, and jitter well, due to the dependence between speech frames.

iLBC is supported for SIP, SCCP, H323, and MGCP devices.

**Note**
H.323 Outbound FastStart does not support the iLBC codec.

• AMR-Adaptive Multi-Rate (AMR) codec is the required standard codec for 2.5G/3G wireless networks based on GSM (WDM, EDGE, GPRS). This codec encodes narrowband (200-3400 Hz) signals at variable bit rates ranging from 4.75 to 12.2 kb/s with toll quality speech starting at 7.4 kbps.

AMR is supported only for SIP devices.

• AMR-WB-Adaptive Multi-Rate Wideband (AMR-WB) is codified as G.722.2, an ITU-T standard speech codec, formally known as Wideband coding of speech for about 16 kb/s. This codec is preferred since it provides excellent speech quality due to a wider speech bandwidth of 50 Hz to 7000 Hz compared to other narrowband speech codecs.

AMR-WB is supported only for SIP devices.

**Note**
AMR-WB is preferred by Cisco Unified Communications Manager over AMR and other supported codecs, G.711 in particular.

The total bandwidth that is used per call stream depends on the audio codec type as well as factors such as data packet size and overhead (packet header size).
Each call includes two streams, one in each direction.

For information on bandwidth usage for each codec, see the Cisco Unified Communications Solution Reference Network Design (SRND) for the current release of Cisco Unified Communications Manager.

Table 5: Bandwidth Used Per Call by Each Codec Type in IPv4

<table>
<thead>
<tr>
<th>Audio Codec</th>
<th>Bandwidth Used for Data Packets Only (Fixed Regardless of Packet Size)</th>
<th>Bandwidth Used Per Call (Including IP Headers) With 30-ms Data Packets</th>
<th>Bandwidth Used Per Call (Including IP Headers) With 20-ms Data Packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>G.711</td>
<td>64 kb/s</td>
<td>80 kb/s</td>
<td>88 kb/s</td>
</tr>
<tr>
<td>G.722</td>
<td>64 kb/s</td>
<td>80 kb/s</td>
<td>88 kb/s</td>
</tr>
<tr>
<td>G.722.1</td>
<td>24 kb/s</td>
<td>Not applicable</td>
<td>40 kb/s</td>
</tr>
<tr>
<td>G.722.1</td>
<td>32 kb/s</td>
<td>Not applicable</td>
<td>48 kb/s</td>
</tr>
<tr>
<td>iSAC</td>
<td>32 kb/s</td>
<td>32 kb/s</td>
<td></td>
</tr>
<tr>
<td>G.723.1</td>
<td>6.3 or 5.3 kb/s</td>
<td>24 kb/s</td>
<td>Not applicable</td>
</tr>
<tr>
<td>G.728</td>
<td>16 kb/s</td>
<td>26.66 kb/s for G.728</td>
<td></td>
</tr>
<tr>
<td>iLBC</td>
<td>15.2 or 13.3 kb/s</td>
<td>24 kb/s for iLBC</td>
<td></td>
</tr>
<tr>
<td>G.729</td>
<td>8 kb/s</td>
<td>24 kb/s</td>
<td>32 kb/s</td>
</tr>
<tr>
<td>L16</td>
<td>256 kb/s</td>
<td>272 kb/s</td>
<td>280 kb/s</td>
</tr>
<tr>
<td>AAC-LD (mpeg4-generic)</td>
<td>256 kb/s</td>
<td>272 kb/s</td>
<td></td>
</tr>
<tr>
<td>AAC-LD (MP4A-LATM)</td>
<td>128 kb/s</td>
<td>Not applicable</td>
<td>156 kb/s¹.</td>
</tr>
<tr>
<td>AAC-LD (MP4A-LATM)</td>
<td>64 kb/s</td>
<td>Not applicable</td>
<td>88 kb/s</td>
</tr>
<tr>
<td>AAC-LD (MP4A-LATM)</td>
<td>56 kb/s</td>
<td>Not applicable</td>
<td>80 kb/s</td>
</tr>
</tbody>
</table>

¹. See footnote 1.
<table>
<thead>
<tr>
<th>Audio Codec</th>
<th>Bandwidth Used for Data Packets Only (Fixed Regardless of Packet Size)</th>
<th>Bandwidth Used Per Call (Including IP Headers) With 30-ms Data Packets</th>
<th>Bandwidth Used Per Call (Including IP Headers) With 20-ms Data Packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAC-LD (LATM)</td>
<td>48 kb/s</td>
<td>Not applicable</td>
<td>72 kb/s</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Note: See footnote 1.</td>
</tr>
<tr>
<td>AAC-LD (MP4A-LATM)</td>
<td>32 kb/s</td>
<td>Not applicable</td>
<td>56 kb/s</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Note: See footnote 1.</td>
</tr>
<tr>
<td>AAC-LD (MP4A-LATM)</td>
<td>24 kb/s</td>
<td>Not applicable</td>
<td>48 kb/s</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Note: See footnote 1.</td>
</tr>
<tr>
<td>GSM (Global system for mobile communications)</td>
<td>13 kb/s</td>
<td>29 kb/s</td>
<td>37 kb/s</td>
</tr>
</tbody>
</table>

1. AAC-LD (MP4A-LATM) does not specify the packetization period (20 ms or 30 ms) in SDP (it assumes the maximum overhead of 24K, which is in 20 ms).

**Simple region configuration example**

The figure below shows a very simple region configuration example for deployment with a central site and two remote branches. In the example, an administrator configures a region for each site, leaving the Max Audio Bit Rate between the regions as Use System Default. Use System Default means that the values of the Service Parameters for the Max Audio Bit Rate are used. The Default Intraregion Max Audio Bit Rate has a factory default value of 64 kbps (G.722, G.711), while the Default Interregion Max Audio Bit Rate has a factory default value of 8 kbps (G.729).
After region configuration, the administrator assigns devices to the following sites:

**Figure 1: Simple region example**

- The Central Campus site to device pools that specify CentralCampus as the region setting
- Remote Site A to device pools that specify RemoteSiteA as the region setting
- Remote Site B to device pools that specify RemoteSiteB for the region setting

**Related Topics**

- Device pools, on page 45
- Locations and regions, on page 70
- System configuration, on page 29

**Add region**

Cisco Unified Communications Manager allows you to add a maximum of 2000 regions.

You must specify the maximum bit rate for devices that are using regions.

**Procedure**

1. Select **System > Service Parameters** in Cisco Unified Communications Manager Administration **Service Parameters Configuration** window to configure the default values for maximum bit rates for audio and video calls.
2. Choose the node.
3. Choose the Cisco Unified Communications Manager service
4. Scroll to the **Clusterwide Parameters (System-Location and Region)** pane
For enhanced scalability and to ensure that the system uses fewer resources, Cisco recommends that you set the default values in the Service Parameters Configuration window for the maximum bit rates for audio and video calls and the link loss type; then, when you configure regions, choose the default settings in the Region Configuration window.

**Step 5** Create regions specifying the maximum bit rates to use for calls within those regions and between other regions.

- For audio calls, the default value within a region is 64 kb/s (which means that G.722 or G.711 may be used for the call, with G.722 being preferred because it has better audio quality).
- For audio calls, the default value between regions is 8 kb/s (G.729).
- For video calls (includes audio), the default value is 384 kb/s.

**Step 6** Create or modify device pools to use the regions that you created.

**Step 7** Assign device pools to devices.

**Step 8** Restart devices to apply any changes to devices that use the updated region.

---

**Device pools**

You can specify the following device characteristics for a device pool:

- **Device Pool Name**—Specifies the name for the new device pool.
- **Date/Time group**—Specifies the date and time zone for a device.
- **Region**—Specifies the audio and video codecs that are used within and between regions. Use regions only if you have different types of codecs within the network.
- **Softkey template**—Manages the softkeys that are associated with applications on Cisco Unified IP Phones.
- **Survivable Remote Site Telephony (SRST) reference**—Specifies the gateway that provides SRST functionality for the devices in a device pool.
- **Calling search space for auto-registration (optional)**—Specifies the partitions that an auto-registered device can reach when a call is placed.
- **Reverted call focus priority (optional)**—Specifies which call type, incoming calls or reverted calls, has priority for user actions, such as going off hook. For example, if a phone has both a reverted call and an incoming call alerting, the incoming call gets retrieved on off hook when incoming calls have priority.
- **Media resource group list (optional)**—Specifies a prioritized list of media resource groups. An application chooses the required media resource (for example, a Music On Hold server, transcoder, or conference bridge) from the available media resource groups according to the priority order that is defined in the media resource group list.
- **Network hold music on hold (MOH) audio sources (optional)**—Specifies the audio source for network hold.
- **User hold music on hold (MOH) audio source (optional)**—Specifies the audio source for user hold.
- **Network locale**—Contains a definition of the tones and cadences that the phones and gateways use in a device pool in a specific geographic area.
You must choose only a network locale that is already installed and that the associated
devices support. The list contains all available network locales for this setting, but not
all are necessarily installed. If the device is associated with a network locale that it does
not support in the firmware, the device will fail to come up.

Note

• Device Mobility Group—Represents the highest level entity that is used to control device mobility for
this device.

• Location—Implements call admission control in a centralized call-processing system.

• Physical Location—Distinguishes the device-mobility-related parameters that apply to a specific
geographical location from other parameters.

• User locale—Identifies a set of detailed information to support users, including language and font. This
characteristic associates with the phones and gateways in a device pool.

• Connection Monitor Duration—Resolves WAN link flapping issues between Cisco Unified Communications
Manager and SRST.

• Single Button Barge/cBarge—Specifies the Single Button Barge/cBarge feature setting.

• Join Across Lines—Specifies the Join Across Lines feature setting.

• Device Mobility Calling Search Space—Specifies the appropriate calling search space to be used as the
device calling search space when the device is roaming and in same device mobility group.

• AAR Calling Search Space—Specifies the calling search space for the device to use when performing
automated alternate routing (AAR).

• AAR Group—Specifies the AAR group for this device. The AAR group provides the prefix digits that
are used to route calls that are otherwise blocked due to insufficient bandwidth. An AAR group setting
of None specifies that no attempt to reroute blocked calls will occur.

• MLPP Precedence and Preemption Information—Manages MLPP settings:
  • MLPP Indication—Specifies whether devices in the device pool that are capable of playing precedence
tones will use the capability when the devices plan an MLPP precedence call.
  • MLPP Preemption—Specifies whether devices in the device pool that are capable of preempting
calls in progress will use the capability when the devices plan an MLPP precedence call.
  • MLPP Domain—Specifies a hexadecimal value for the MLPP domain that is associated with the
device pool. Device pools refer to the configured MLPP domain.

• Calling Party Transformation Pattern CSS and international escape character + (prefix) settings.

Note

You must configure the preceding items before you configure a device pool if you want to choose the
items for the device pool.

After you add a new device pool to the database, you can use it to configure devices such as Cisco Unified
IP Phones, gateways, conference bridges, transcoders, media termination points, voice-mail ports, and CTI
route points.
If you are using auto-registration, you can assign all devices of a given type to a device pool by using the Device Defaults window in Cisco Unified Communications Manager Administration.

Related Topics
- Autoregistration overview, on page 126
- Date/time groups, on page 35
- Regions, on page 37
- Call Admission Control, on page 48
- Survivable Remote Site Telephony references, on page 49
- Partitions and calling search spaces, on page 135
- Understanding route plans, on page 143
- Use the international escape character, on page 161
- Directory numbers, on page 191
- Media resource group lists, on page 253
- System configuration, on page 29

Update device pools

If you make changes to a device pool, you must reset the devices in that device pool before the changes will take effect.

You cannot delete a device pool that has been assigned to any devices or one that is used for Device Defaults configuration.

If you try to delete a device pool that is in use, a message displays. Before deleting a device pool that is currently in use, you must perform either or both of the following tasks:

- Update the devices to assign them to a different device pool.
- Delete the devices that are assigned to the device pool that you want to delete.

See the Local route groups and called party transformations, on page 151 for an explanation of local route groups and the details of provisioning route groups, device pools, route lists, partitions, route patterns, and calling search spaces in a local route group scenario.

Procedure

Step 1  To find out which devices are using the device pool, choose Dependency Records from the Related Links drop-down list box on the Device Pool Configuration window.

Step 2  Click Go.

Common device configuration

A common device configuration comprises user-specific service and feature attributes. You can specify the following device characteristics for a common device configuration:

- Name-Specifies the name for the common device configuration.
• Softkey Template-Specifies the softkey template that is associated with the devices in the device pool.
• User Hold MOH Audio Source-Specifies the audio source to use for music on hold (MOH) when a user initiates a hold action.
• Network Hold MOH Audio Source-Specifies the audio source to use for MOH when the network initiates a hold action.
• User Locale-Specifies the location that is associated with the phones and gateways in the device pool.
• MLPP Indication-Specifies whether devices in the device pool that are capable of playing precedence tones will use the capability when the devices place an MLPP precedence call.
• MLPP Preemption-Specifies whether devices in the device pool that are capable of preempting calls in progress will use the capability when the devices place an MLPP precedence call.
• MLPP Domain-Specifies the MLPP domain that is associated with this device pool.

LDAP

See the Directory overview, on page 225 chapter for information about using directories with Cisco Unified Communications Manager.

Call Admission Control

Use call admission control to maintain a desired level of voice quality over a WAN link. For example, you can use call admission control to regulate the voice quality on a 56-kb/s frame relay line that connects your main campus and a remote site.

Voice quality can begin to degrade when too many active calls exist on a link and the amount of bandwidth is oversubscribed. Call admission control regulates voice quality by limiting the number of calls that can be active at the same time on a particular link. Call admission control does not guarantee a particular level of audio quality on the link, but it does allow you to regulate the amount of bandwidth that active calls on the link consume.

Cisco Unified Communications Manager supports two types of call admission control:

• Locations-Use locations to implement call admission control in a centralized call-processing system. Call admission control lets you regulate voice quality by limiting the amount of bandwidth that is available for calls over links between the locations.

Note

If you do not use call admission control to limit the voice bandwidth on an IP WAN link, the system allows an unlimited number of calls to be active on that link at the same time. This can cause the voice quality of each call to degrade as the link becomes oversubscribed.

Related Topics

Device pools, on page 45
Locations and regions, on page 36
Survivable Remote Site Telephony references

Survivable Remote Site Telephony (SRST) gets used at sites that depend on a Cisco Unified Communications Manager that is accessible via a WAN connection. SRST provides telephony service to IP phones at the remote site in the event of a WAN outage. An SRST-enabled router has features that allow calls between IP phones at the remote site to call each other, allow calls from the PSTN to reach the IP phones, and allow calls from the IP phones to reach the external world through the PSTN. Intelligence in the SRST router that can accept registrations from the IP phones and route calls based on the directory numbers that are registered, and based on the routing that is configured for the PSTN link, accomplishes that.

Survivable remote site telephony (SRST) references, a configurable option in Cisco Unified Communications Manager Administration, provide limited call capability in the event of a WAN outage. Using SRST references, IP gateways can take over limited Cisco Unified Communications Manager functionality. When phones lose connectivity to all associated Cisco Unified Communications Managers, the phones in a device pool attempt to make a Cisco Unified Communications Manager connection to the SRST reference IP gateway.

The status line indication on the IP phone that shows the phone has failed over to the backup proxy (SRST gateway) provides the only user interactions with SRST.

Device Pool Settings for SRST

The system administrator can configure the SRST configuration for a device pool of phones. The following list gives Device Pool configuration options that are available:

- **Disable**– If a phone cannot reach any Cisco Unified Communications Managers, it does not try to connect to an SRST gateway.
- **Use Default Gateway**– If a phone cannot reach any Cisco Unified Communications Managers, it tries to connect to its IP gateway as an SRST gateway.
- **User-defined**– If a phone cannot reach any Cisco Unified Communications Managers, it tries to connect to an administrator-specified SRST gateway. The SRST Reference field of the Device Pool Configuration lists user-defined SRST references.

The administrator defines SRST configurations in the SRST Reference Configuration window. Any preceding SRST configuration option can apply to a device pool. The Cisco TFTP reads the SRST configuration and provides it to the IP phone in a .cnf.xml file. The IP phone reacts appropriately to the SRST configuration.

Connection Monitor Duration

An IP phone that connects to the SRST over a Wide Area Network (WAN) reconnects itself to Cisco Unified Communications Manager as soon as it can establish a connection with Cisco Unified Communications Manager over the WAN link. However, if the WAN link is unstable, the IP phone switches back and forth between the SRST and Cisco Unified Communications Manager. This situation causes 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 to Cisco Unified Communications Manager. These WAN link disruptions fit into two classifications: infrequent random outages that occur on an otherwise stable WAN and the sporadic, frequent disruptions that last a few minutes.

To resolve the WAN link flapping issues between Cisco Unified Communications Manager and SRST, Cisco Unified Communications Manager provides an enterprise parameter and a setting in the Device Pool Configuration window that is called Connection Monitor Duration. Depending upon system requirements, the administrator decides which parameter to use. The value of the parameter gets delivered to the IP phone in the XML configuration file.
• The default for the enterprise parameter specifies 120 seconds. Use the enterprise parameter to change
the connection duration monitor value for all IP phones that are configured in Cisco Unified
Communications Manager Administration.

• Use the Device Pool Configuration window to change the connection duration monitor value for all IP
phones in a specific device pool.

**SRST Reference Configuration Options for Phones That Are Running SIP**

A remote site may have a mix of SCCP and SIP endpoints in addition to PSTN gateway access. For calls to
be routed between the different protocols and the PSTN, three different features will get configured in one
SRST router that will allow calls to be routed between phones that are running SCCP, phones that are running
SIP, and the PSTN during a WAN outage. In addition, the SRST Reference Configuration window in Cisco
Unified Communications Manager Administration provides two fields:

- **SIP Network/IP Address**—The SIP network/IP address applies for SIP SRST. This address notifies the
  phone that is running SIP where to send SIP Register message for SIP SRST.

- **SIP Port**—SIP port of the SRST gateway. Default specifies 5060.

For more information, see [System-level configuration settings](#), on page 29.

For information about configuring security for the SRST reference and the SRST-enabled gateway, see the
Cisco Unified Communications Manager Security Guide.

**Related Topics**

- Device pools, on page 45
- System configuration, on page 29

**MLPP domain**

Because the MLPP service applies to a domain, Cisco Unified Communications Manager only marks a
precedence level to connections and resources that belong to calls from MLPP users in a given domain. The
MLPP domain subscription of the originating user determines the domain of the call and its connections. Only
higher precedence calls in one domain can preempt connections that calls in the same domain are using.

To define an MLPP domain, configure the following MLPP domain information:

- **Domain Name-Name** of the MLPP domain.

- **Domain Identifier**—Configure the MLPP domain identifier as a hexadecimal value of zero or greater (the
default value specifies zero).

The MLPP domain identifier comprises the collection of devices and resources that are associated with an
MLPP subscriber. When an MLPP subscriber (who belongs to a particular domain) places a precedence call
to another MLPP subscriber (who belongs to the same domain), the MLPP service can preempt the existing
call that the called MLPP subscriber is on for a higher precedence call. The MLPP service availability does
not cross domains. Device pools refer to the configured MLPP domain.

**Note**

You must reset all devices for a change to this setting to take effect.
Enterprise parameters

Enterprise parameters provide default settings that apply to all devices and services. When you install a new Cisco Unified Communications Manager, it uses the enterprise parameters to set the initial values of its device defaults.

You cannot add or delete enterprise parameters, but you can update existing enterprise parameters. Cisco Unified Communications Manager Administration divides enterprise parameters by categories; for example, CCMAdmin parameters, CCMUser parameters, and CDR parameters.

You can display additional descriptions for enterprise parameters by using the question mark button on the Enterprise Parameters Configuration window.

Related Topics

System configuration, on page 29

Service parameters

Service parameters for Cisco Unified Communications Manager allow you to configure different services on selected servers. You can view a list of parameters and their descriptions by clicking the question mark button that displays on the Service Parameters Configuration window. You can view the list with a particular parameter at the top by clicking that parameter.

If you deactivate a service by using Cisco Unified Serviceability, Cisco Unified Communications Manager retains any updated service parameter values. If you start the service again, Cisco Unified Communications Manager sets the service parameters to the changed values.

Caution

Some changes to service parameters may cause system failure. Cisco recommends that you do not make any changes to service parameters unless you fully understand the feature that you are changing or unless the Cisco Technical Assistance Center (TAC) requests that you make changes.

Related Topics

System configuration, on page 29

Dependency records

Use dependency records to find specific information about system-level settings such as servers, device pools, and date/time groups.
Procedure

**Step 1** Choose *Dependency Records* from the *Related Links* drop-down list box on the Cisco Unified Communications Manager Administration configuration windows for each system-level setting.

**Step 2** Click *Go*.

If the dependency records are not enabled for the system, the dependency records summary window displays a message.

**Note**
You cannot view dependency records from the *Device Defaults* and *Enterprise Parameters Configuration* windows.

The *Cisco Unified CM Configuration Dependency Records* window provides information about Cisco Unified Communications Manager groups that it accesses. The *Date/Time Group Configuration Dependency Records* window provides information about device pools that it accesses.

**Related Topics**

- System-level configuration settings, on page 29
- System configuration, on page 29
CHAPTER 6

Clustering

This chapter provides information about the clustering feature of Cisco Unified Communications Manager which provides a mechanism for distributing call processing and database replication amongst multiple Cisco Unified Communications Manager servers that run the exact same version of Cisco Unified Communications Manager. Clustering provides transparent sharing of resources and features and enables system scalability.

- Configure cluster, page 53
- Clusters, page 54
- Database replication in a cluster, page 54
- Intercluster communication, page 55
- Balanced call processing, page 56

Configure cluster

This topic provides an overview of the steps that are required to install and configure a Cisco Unified Communications Manager cluster, which comprises a set of Cisco Unified Communications Manager servers that share the same database and resources.

Procedure

**Step 1** Gather the information that you need to install Cisco Unified Communications Manager and any other software applications on the first node and subsequent servers. Also, determine how you will allocate the servers in the cluster.

**Step 2** Install the database server (first node). See the installation documentation for the hardware components that you are installing.

**Step 3** Install Cisco Unified Communications Manager and any additional software applications on the subsequent servers.

**Note** Before installing the subsequent servers, you must define the nodes in the Server Configuration window in Cisco Unified Communications Manager Administration.
Step 4 Configure device pools and use them to assign specific devices to a Cisco Unified Communications Manager group.

Step 5 If you are using an intercluster trunk, install and configure it as an intercluster trunk, either gatekeeper-controlled or non-gatekeeper-controlled.

Step 6 If you want to provide call admission control for an intercluster trunk, configure either a gatekeeper-controlled intercluster trunk or Cisco Unified Communications Manager locations.

Clusters

A cluster comprises a set of Cisco Unified Communications Manager servers that share the same database and resources. You can configure the servers in a cluster in various ways to perform the following functions:

- Database replication
- TFTP server
- Application software server

You can use various nodes in the cluster for call-processing redundancy and for load balancing. You can activate feature services on various nodes in the cluster to specify which servers perform certain functions for the cluster. By accessing the Service Activation window in Cisco Unified Serviceability, you can dedicate a particular server to one function or combine several functions on one server, depending on the size of your system and the level of redundancy that you want.

Tip

The Restart Cisco Communications Manager on Initialization Exception service parameter determines whether the Cisco CallManager service restarts if an error occurs during initialization. This parameter defaults to TRUE and, with this value, the Cisco Communications Manager initialization aborts when an error occurs during initialization. Setting the value to FALSE allows initialization to continue when an error is encountered. You can locate this clusterwide parameter in the

Database replication in a cluster

A cluster comprises a set of Cisco Unified Communications Managers servers that share a common database. When you install and configure Cisco Unified Communications Manager, you specify which servers belong to the same cluster. A cluster comprises the first node (publisher) and subsequent nodes (subscribers). The first node in a cluster contains the Cisco Unified Communications Manager database, which gets automatically installed when you install Cisco Unified Communications Manager on the first node. Cisco Unified Communications Manager uses all subsequent nodes in the cluster for database replication. After you add the subsequent node to the Server Configuration window in Cisco Unified Communications Manager Administration and install Cisco Unified Communications Manager on the subsequent node, the node contains a replicate of the database that exists on the first node.

After you add, update, or delete configuration in Cisco Unified Communications Manager Administration, Cisco Unified Serviceability, or Cisco Unified CM User Options, Cisco Unified Communications Manager writes the configuration update to the Cisco Unified Communications Manager database on the first node in the cluster and then updates the database replicates on the subsequent nodes. If both the first node and
subsequent nodes are available, you read and write configuration data in the GUIs on the first node, even when you browse to GUIs on the subsequent node(s) in the cluster. If the first node is unavailable, you can read configuration data in the GUIs on the subsequent node(s), but you cannot make updates in the GUIs on the subsequent nodes.

Consider the following information that is related to Cisco Unified Communications Manager database replication:

- Before you install Cisco Unified Communications Manager on the subsequent node, you must add the subsequent node to the Server Configuration window by accessing Cisco Unified Communications Manager Administration on the first node. For more information on adding a subsequent node to Cisco Unified Communications Manager Administration, see Balanced call processing, on page 56.

- For Cisco Unified Communications Manager database replication to occur, you must install the exact same version of Cisco Unified Communications Manager on the first node and subsequent node(s) in the cluster.

- Do not make configuration changes (additions, updates, or deletions) during a Cisco Unified Communications Manager upgrade. If you make configuration changes during an upgrade, you may cause data to be lost or cause data not to replicate; in addition, the upgrade may fail.

- You can view the Unified CM Cluster Overview report in Cisco Unified Reporting to determine how all nodes are classified in the database; that is, if the node serves as the first (publisher) or a subsequent (subscriber) node. Likewise, you can click the Host Name/IP Address link in the Find and List Servers window in Cisco Unified Communications Manager Administration; after the Server Configuration window displays, you can view the read-only Database Replication field. If the field displays Publisher, the node serves as the first node. If the field displays Subscriber, the node serves as a subsequent node.

- Changing the name or IP address of a node in a cluster impacts Cisco Unified Communications Manager database replication. Before you change the name or IP address of a node, review the document, Changing the IPAddress and HostName for Cisco Unified Communications Manager Release 8.5(1).

- To verify the state of Cisco Unified Communications Manager database replication, for example, whether replication is occurring, broken, and so on, you can use the Real-Time Monitoring Tool, Cisco Unified Reporting, or the Command Line Interface (CLI).

- If you determine that a problem exists with Cisco Unified Communications Manager database replication, you can repair database replication via the Command Line Interface (CLI).

- If you revert to a previous version of Cisco Unified Communications Manager, you must reset Cisco Unified Communications Manager database replication via the Command Line Interface (CLI) after you revert to the previous version.

### Intercluster communication

In very large environments, you might need to configure more than one cluster to handle the call-processing load. Communication between the clusters typically occurs by means of intercluster trunks or gatekeeper trunks. Most large systems use one of two main types of multicluster configurations:

- Large, single campus, or metropolitan-area network (MAN)
- Multisite WAN with distributed call processing (one or more Cisco Unified Communications Managers at each site)
Because intercluster trunks in a MAN usually have sufficient bandwidth, they do not require any call admission control mechanism. Multisite WANs with distributed call processing typically use gatekeeper technology for call admission control.

**Intracluster Communication**

Cisco Unified Communications Manager also supports intracluster communication, which is a multisite WAN with centralized call processing (no Cisco Unified Communications Manager at the remote site or sites). Multisite WANs with centralized call processing use the locations feature in Cisco Unified Communications Manager to implement call admission control.

Most features of Cisco Unified Communications Manager do not extend beyond a single cluster, but the following features do exist between clusters:

- Basic call setup
- G.711 and G.729 calls
- Multiparty conference
- Call hold
- Call transfer
- Call park
- Calling line ID

For more information about intercluster communication and call admission control, see Cisco Unified Communications Solution Reference Network Design (SRND).

**Balanced call processing**

After installing the Cisco Unified Communications Managers that form a cluster, you should, as much as possible, evenly balance the call-processing load across the system by distributing the devices (such as phones, gateways, CTI route points, CTI ports, and route lists) among the various Cisco Unified Communications Managers in the cluster. To distribute the devices, you configure Cisco Unified Communications Manager groups and device pools and then assign the devices to the device pools in a way that achieves the balance that you want.

Cisco Unified Communications Manager groups and device pools represent logical groupings of devices that you can arrange in any way that you want. For ease of administration, make sure that all the devices in a group or pool share a common and easily identified characteristic, such as their physical location on the network.

You can also use Cisco Unified Communications Manager groups to establish redundancy (backup call processors) for the primary Cisco Unified Communications Manager in the group. A Cisco Unified Communications Manager group comprises an ordered list of up to three Cisco Unified Communications Manager servers. During normal operation, the first (primary) Cisco Unified Communications Manager in the group controls all device pools and devices that are assigned to that group. If the primary Cisco Unified Communications Manager in a group fails, control of the device pools and devices that are registered with the primary Cisco Unified Communications Manager transfers to the next Cisco Unified Communications Manager in the group list.

For example, assume a simplified system that comprises three Cisco Unified Communications Managers in a cluster, with 300 existing Cisco Unified IP Phones and provisions to auto-register new phones as they are added later.
• The configuration includes four Cisco Unified Communications Manager groups: group G1 that is assigned to device pool DP1, group G2 that is assigned to device pool DP2, group G3 that is assigned to device pool DP3, and group G4 that is assigned to device pool DP4. Group G4 serves as the default group for devices that auto-register.

• Unified CM1 serves as the primary Cisco Unified Communications Manager for the devices in DP1 and DP2, first backup for DP3, and second backup for the devices in DP4.

• Unified CM2 serves as the primary Cisco Unified Communications Manager for the devices in DP3 and DP2, first backup for DP1, and second backup for the devices in DP2.

• Unified CM3 serves as the first backup Cisco Unified Communications Manager for the devices in DP2 and DP4 and second backup for the devices in DP1 and DP3.

**Related Topics**

NTP reference configuration, on page 35
Balanced call processing
Redundancy

This chapter provides information about redundancy in Cisco Unified Communications Manager which provides several forms of redundancy:

- Call-processing redundancy—Using Cisco Unified Communications Manager groups, you can designate backup Cisco Unified Communications Managers to handle call processing for a disabled Cisco Unified Communications Manager in a form of redundancy known as device failover.
- Media resource redundancy
- CTI redundancy

- Cisco Unified Communications Manager redundancy groups, page 59
- Media resource redundancy, page 62
- CTI redundancy, page 63

Cisco Unified Communications Manager redundancy groups

Groups and clusters form logical collections of Cisco Unified Communications Managers and their associated devices. Groups and clusters do not necessarily relate to the physical locations of any of their members.

A cluster comprises a set of Cisco Unified Communications Managers that share a common database. When you install and configure Cisco Unified Communications Manager, you specify which servers belong to the same cluster. For information on database replication in a cluster, see the Database replication in a cluster, on page 54.

A group comprises a prioritized list of up to three Cisco Unified Communications Managers. You can associate each group with one or more device pools to provide call-processing redundancy. You use Cisco Unified Communications Manager Administration to define the groups, to specify which Cisco Unified Communications Managers belong to each group, and to assign a Cisco Unified Communications Manager group to each device pool.

Cisco Unified Communications Manager groups

A Cisco Unified Communications Manager group comprises a prioritized list of up to three Cisco Unified Communications Managers. Each group must contain a primary Cisco Unified Communications Manager,
Cisco Unified Communications Manager redundancy groups

and it may contain one or two backup Cisco Unified Communications Managers. The order in which you list the Cisco Unified Communications Managers in a group determines the priority order.

Cisco Unified Communications Manager groups provide both redundancy and recovery:

- **Failover**—Occurs when the primary Cisco Unified Communications Manager in a group fails, and the devices reregister with the backup Cisco Unified Communications Manager in that group.
- **Fallback**—Occurs when a failed primary Cisco Unified Communications Manager comes back into service, and the devices in that group reregister with the primary Cisco Unified Communications Manager.

Under normal operation, the primary Cisco Unified Communications Manager in a group controls call processing for all the registered devices (such as phones and gateways) that are associated with that group. If the primary Cisco Unified Communications Manager fails for any reason, the first backup Cisco Unified Communications Manager in the group takes control of the devices that were registered with the primary Cisco Unified Communications Manager. If you specify a second backup Cisco Unified Communications Manager for the group, it takes control of the devices if both the primary and the first backup Cisco Unified Communications Managers fail.

When a failed primary Cisco Unified Communications Manager comes back into service, it takes control of the group again, and the devices in that group automatically reregister with the primary Cisco Unified Communications Manager.

You associate devices with a Cisco Unified Communications Manager group by using device pools. You can assign each device to one device pool and associate each device pool with one Cisco Unified Communications Manager group. You can combine the groups and device pools in various ways to achieve the desired level of redundancy.

**Note**

A server can exist in a single device pool and can support up to 7500 devices (high-end servers only). Contact your Cisco representative for information on the types of servers that Cisco Unified Communications Manager supports.

For example, the following figure shows a simple system with three Cisco Unified Communications Managers in a single group that is controlling 800 devices.

**Figure 2: Cisco Unified Communications Manager Group**

The figure depicts Cisco Unified Communications Manager group G1 that is assigned with two device pools, DP1 and DP2. Cisco Unified Communications Manager 1, as the primary Cisco Unified Communications Manager in group G1, controls all 800 devices in DP1 and DP2 under normal operation. If Cisco Unified Communications Manager 1 fails, control of all 800 devices transfers to Cisco Unified Communications
Manager 2. If Cisco Unified Communications Manager 2 also fails, control of all 800 devices transfers to Cisco Unified Communications Manager 3.

The configuration provides call-processing redundancy, but it does not distribute the call-processing load very well among the three Cisco Unified Communications Managers in the example. For information on load balancing, see the Distributing devices for redundancy and load balancing, on page 61.

---

**Note**

Empty Cisco Unified Communications Manager groups will not function.

---

**Distributing devices for redundancy and load balancing**

Cisco Unified Communications Manager groups provide both call-processing redundancy and distributed call processing. How you distribute devices, device pools, and Cisco Unified Communications Managers among the groups determines the level of redundancy and load balancing in your system.

In most cases, you would want to distribute the devices in a way that prevents the other Cisco Unified Communications Managers from becoming overloaded if one Cisco Unified Communications Manager in the group fails. The following figure shows one possible way to configure the Cisco Unified Communications
Manager groups and device pools to achieve both distributed call processing and redundancy for a system of three Cisco Unified Communications Managers and 800 devices.

**Figure 3: Redundancy Combined with Distributed Call Processing**

The previous figure depicts the Cisco Unified Communications Manager groups as they are configured and assigned to device pools, so Cisco Unified Communications Manager 1 serves as the primary controller in two groups, G1 and G2. If Cisco Unified Communications Manager 1 fails, the 100 devices in device pool DP1 reregister with Cisco Unified Communications Manager 2, and the 300 devices in DP2 reregister with Cisco Unified Communications Manager 3. Similarly, Cisco Unified Communications Manager 2 serves as the primary controller of groups G3 and G4. If Cisco Unified Communications Manager 2 fails, the 100 devices in DP3 reregister with Cisco Unified Communications Manager 1, and the 300 devices in DP4 reregister with Cisco Unified Communications Manager 3. If Cisco Unified Communications Manager 1 and Cisco Unified Communications Manager 2 both fail, all devices reregister with Cisco Unified Communications Manager 3.

For more information on distributed call processing, see the Balanced call processing, on page 56.

**Media resource redundancy**

Media resource lists provide media resource redundancy by specifying a prioritized list of media resource groups. An application can select required media resources from among the available ones according to the
priority order that is defined in the media resource list. For more information on media resource redundancy, see the Media resource management, on page 245.

CTI redundancy

Computer telephony integration (CTI) provides an interface between computer-based applications and telephony functions. CTI uses various redundancy mechanisms to provide recovery from failures in any of the following major components:

- Cisco Unified Communications Manager
- Cisco CTI Manager
- Applications that use CTI

CTI uses Cisco Unified Communications Manager redundancy groups to provide recovery from Cisco Unified Communications Manager failures. To handle recovery from failures in Cisco CTI Manager itself, CTI allows you to specify primary and backup Cisco CTI Managers for the applications that use CTI. Finally, if an application fails, the Cisco CTI Manager can redirect calls that are intended for that application to a forwarding directory number.
Call admission control

This chapter provides information about call admission control which enables you to control the audio quality and video quality of calls over a wide-area (IP WAN) link by limiting the number of calls that are allowed on that link at the same time. For example, you can use call admission control to regulate the voice quality on a 56-kb/s frame relay line that connects your main campus and a remote site.

Audio and video quality can begin to degrade when too many active calls exist on a link and the amount of bandwidth is oversubscribed. Call admission control regulates audio and video quality by limiting the number of calls that can be active on a particular link at the same time. Call admission control does not guarantee a particular level of audio or video quality on the link, but it does allow you to regulate the amount of bandwidth that active calls on the link consume.

Call admission control operates by rejecting a call for bandwidth and policy reasons. When a call gets rejected due to call admission control, the phone of the called party does not ring, and the caller receives a busy tone. The caller also receives a message on their phone, such as “Not enough bandwidth.”

Without call admission control, you may perceive that IP voice is low in quality and unreliable. With call admission control, customers experience situations similar to the time-division multiplexing (TDM) processing and realize that they need more bandwidth for peak hours.

This section describes two types of call admission control that you can use with Cisco Unified Communications Manager:

• Locations, on page 68, for systems with centralized call processing
• Configure gatekeepers and trunks, on page 74, for systems with distributed call processing

You can choose either of these methods of call admission control, but you cannot combine them in the same Cisco Unified Communications Manager system. If your system does not contain IP WAN links with limited available bandwidth, you do not have to use call admission control.

Cisco Unified Communications Manager also supports Resource Reservation Protocol (RSVP), an additional CAC mechanism that offers additional capabilities for full-mesh network topologies.

• Configure locations, page 66
• Configure gatekeeper and gatekeeper-controlled trunk, page 67
• Locations, page 68
• Configure gatekeepers and trunks, page 74
Configure locations

Locations, which are available in Cisco Unified Communications Manager, provide call admission control for centralized call-processing systems. Call admission control enables you to control the audio quality and video quality of calls over a wide-area (IP WAN) link by limiting the number of calls that are allowed on that link at the same time. For example, you can use call admission control to regulate the voice quality on a 56-kb/s frame relay link that connects your main campus and a remote site.

Audio and video quality can begin to degrade when too many active calls exist on a link and the amount of bandwidth is oversubscribed. Call admission control regulates audio and video quality by limiting the number of calls that can be active on a particular link at the same time. Call admission control does not guarantee a particular level of audio or video quality on the link, but it does allow you to regulate the amount of bandwidth that active calls on the link consume.

Call admission control operates by rejecting a call for bandwidth and policy reasons. When a call gets rejected due to call admission control, the phone of the called party does not ring, and the caller receives a busy tone. The caller also receives a message on their phone, such as “Not enough bandwidth.”

Without call admission control, you may perceive that IP voice is low in quality and unreliable. With call admission control, you may experience situations similar to the time-division multiplexing (TDM) processing and realize that they need more bandwidth for peak hours. If your system does not contain IP WAN links with limited available bandwidth, you do not have to use call admission control.

A centralized system uses a single Cisco Unified Communications Manager cluster to control all the locations. You can choose to configure locations or to configure gatekeepers and trunks for call admission control, but you cannot combine them in the same Cisco Unified Communications Manager system.

---

**Note**

For non-centralized systems, Cisco Unified Communications Manager offers an alternative CAC method, Resource Reservation Protocol (RSVP).

**Tip**

Do not confuse locations with geolocations. Locations, which you configure by using the System > Location menu option, allow you to define entities that a centralized call-processing system uses to provide call admission control (CAC). Geolocations, which you configure by using the System > Geolocation Configuration menu option, allow you to specify geographic locations that you use to associate Cisco Unified Communications Manager devices for features such as logical partitioning.

The general steps for configuring call admission control on the basis of locations is as follows.

**Procedure**

**Step 1** Configure a region for each type of codec that is used in your system.

**Step 2** Configure a separate location for each IP WAN link to which you want to apply call admission control. Allocate the maximum available bandwidth for calls across the link to that location.

**Note** If you set the bandwidth to Unlimited, you allocate unlimited available bandwidth and allow an unlimited number of active calls on the IP WAN link for that location.

**Step 3** Configure the device pools for your system and choose the appropriate region for each.

**Step 4** Configure the phones and other devices and assign each of them to the appropriate device pool and location.
If you set the location to Hub_None, you assign that device to an unnamed location with unlimited available bandwidth and allow an unlimited number of active calls to and from that device.

**Related Topics**

- Locations, on page 68
- Locations and regions, on page 70
- Resource Reservation Protocol, on page 79
- Cisco Unified IP phones, on page 459

## Configure gatekeeper and gatekeeper-controlled trunk

Call admission control enables you to control the audio quality and video quality of calls over a wide-area (IP WAN) link by limiting the number of calls that are allowed on that link at the same time. For example, you can use call admission control to regulate the voice quality on a 56-kb/s frame relay line that connects your main campus and a remote site.

Audio and video quality can begin to degrade when too many active calls exist on a link and the amount of bandwidth is oversubscribed. Call admission control regulates audio and video quality by limiting the number of calls that can be active on a particular link at the same time. Call admission control does not guarantee a particular level of audio or video quality on the link, but it does allow you to regulate the amount of bandwidth that active calls on the link consume.

Call admission control operates by rejecting a call for bandwidth and policy reasons. When a call gets rejected due to call admission control, the phone of the called party does not ring, and the caller receives a busy tone. The caller also receives a message on their phone, such as “Not enough bandwidth.”

Without call admission control, you may perceive that IP voice is low in quality and unreliable. With call admission control, you may experience situations similar to the time-division multiplexing (TDM) processing and realize that they need more bandwidth for peak hours. If your system does not contain IP WAN links with limited available bandwidth, you do not have to use call admission control.

Gatekeeper call admission control provides great flexibility:

- Gatekeepers reduce configuration overhead by eliminating the need to configure a separate H.323 device for each remote Cisco Unified Communications Manager that is connected to the IP WAN.
- A gatekeeper can determine the IP addresses of devices that are registered with it, or you can enter the IP addresses explicitly.
- The gatekeeper supports the H.323 protocol and uses the H.225 protocol to make calls.
- The gatekeeper can perform basic call routing in addition to call admission control.

**Note**

See the *Cisco Unified Communications Solution Reference Network Design (SRND)* for more detailed information about gatekeeper configuration, dial plan considerations when a gatekeeper is used, and gatekeeper interaction with Cisco Unified Communications Manager.
Procedure

Step 1  On the gatekeeper device, configure the appropriate zones and bandwidth allocations for the various Cisco Unified Communications Managers that will route calls to it. See “Configuring H.323 Gatekeepers and Proxies”, Cisco IOS H.323 Configuration Guide

Step 2  Configure gatekeeper settings in Cisco Unified Communications Manager Administration. Repeat this step for each Cisco Unified Communications Manager that will register with the gatekeeper. Make sure Host Name or IP Address is set the same way on each Cisco Unified Communications Manager.

Step 3  Configure the appropriate intercluster trunks or H.225 trunks to specify gatekeeper information (if gatekeeper-controlled).

Step 4  Configure a route pattern to route calls to each gatekeeper-controlled trunk.

Related Topics

- Gateways dial plans and route groups, on page 374
- Configure gatekeepers and trunks, on page 74
- Understanding route plans, on page 143

Locations

The locations feature, which is available in Cisco Unified Communications Manager, provides call admission control for centralized call-processing systems. A centralized system uses a single Cisco Unified Communications Manager cluster to control all the locations. For non-centralized systems, Cisco Unified Communications Manager offers an alternative CAC method, Resource Reservation Protocol (RSVP). See for a description of RSVP.

Tip

Do not confuse locations with geolocations. Locations, which you configure by using the System > Location menu option, allow you to define entities that a centralized call-processing system uses to provide call admission control (CAC). Geolocations, which you configure by using the System > Geolocation Configuration menu option, allow you to specify geographic locations that you use to associate Cisco Unified Communications Manager devices for features such as logical partitioning.
In a centralized call-processing system, as illustrated here, the Cisco Unified Communications Manager cluster resides at the main location, along with other devices such as phones and gateways.

Figure 4: Call admission control that uses locations in a centralized system

The remote locations (for example, branch offices of your company) house additional phones and other devices, but they do not contain any call-processing capability. The remote locations connect to the main location by means of IP WAN links (and possibly PSTN and ISDN links as backups) and to each other by going through the main location (central campus).

Calls between devices at the same location do not need call admission control because those devices reside on the same LAN, which has unlimited available bandwidth. However, calls between devices at different locations must travel over an IP WAN link, which has limited available bandwidth.

The locations feature in Cisco Unified Communications Manager lets you specify the maximum amount of audio bandwidth (for audio calls) and video bandwidth (for video calls) that is available for calls to and from each location, which thereby limits the number of active calls and limits oversubscription of the bandwidth on the IP WAN links.

Each audio call includes two streams, one in each direction. Video calls have four or six streams (that is, two or three streams in each direction).

Location example

For example, assume that you have configured the following locations in Cisco Unified Communications Manager Administration:

<table>
<thead>
<tr>
<th>Location</th>
<th>Bandwidth (kb/s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>San Francisco (main location)</td>
<td>Unlimited</td>
</tr>
</tbody>
</table>
Bandwidth (kb/s)

<table>
<thead>
<tr>
<th>Location</th>
<th>Bandwidth (kb/s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Austin (remote location)</td>
<td>160</td>
</tr>
<tr>
<td>Dallas (remote location)</td>
<td>200</td>
</tr>
</tbody>
</table>

Cisco Unified Communications Manager continues to admit new calls to a link as long as sufficient bandwidth is still available. Thus, if the link to the Austin location in the example has 160 kb/s of available bandwidth, that link can support two G.711 calls at 80 kb/s each, six G.723 or G.729 calls at 24 kb/s each, or five GSM calls at 29 kb/s each. If any additional calls try to exceed the bandwidth limit, the system rejects them, the calling party receives reorder tone, and a text message displays on the phone.

**Audio bandwidth**

When you configure a location in Cisco Unified Communications Manager Administration, you assign it a name and maximum audio bandwidth. If you set the audio or video bandwidth to Unlimited, you allocate unlimited available bandwidth and allow an unlimited number of active calls on the IP WAN link for that location. In configuring a location, you also assign a video bandwidth for the location. If you set the video bandwidth setting to None, no video calls can connect between this location and other locations, but they can take place within this location.

When you configure a phone or other device in Cisco Unified Communications Manager Administration, you can assign it to a location. If you set the location to Hub_None, you assign that device to an unnamed location with unlimited available bandwidth and allow an unlimited number of active calls to and from that device.

Location reservations move to reflect the type of call. When a call changes from video to audio-only, the location reservation moves from the video location to an audio location. Calls that change from audio-only to video cause the opposite change of location reservation.

**Related Topics**

- Resource Reservation Protocol, on page 79
- Configure locations, on page 66

**Locations and regions**

Locations work in conjunction with regions to define the characteristics of a network link. Regions define the type of compression (G.711, G.722, G.723, G.729, GSM, or wideband) that is used on the link, and locations define the amount of available bandwidth for the link. You assign each device in the system to both a region (by means of a device pool) and a location.
As illustrated here, the regions and locations can overlap and intersect in various ways, depending on how you define them.

**Figure 5: Interaction among locations and regions**

---

**Bandwidth calculations**

In performing location bandwidth calculations for purposes of call admission control, Cisco Unified Communications Manager assumes that each call stream consumes the following amount of bandwidth:

- G.711 call uses 80 kb/s.
- G.722 call uses 80 kb/s.
- G.723 call uses 24 kb/s.
- G.728 call uses 26.66 kb/s.
- G.729 call uses 24 kb/s.
- GSM call uses 29 kb/s.
- Wideband call uses 272 kb/s.
- iLBC call uses 24 kb/s.
- AMR call uses 12.2 kb/s.
- AMR-WB call uses 23.85 kb/s.
- AAC call uses value that video mline specifies.
Each audio call comprises two call streams. Actual bandwidth consumption per call varies, depending on factors such as data packet size. Cisco Unified Communications Manager uses these fixed values to simplify the bandwidth calculations for purposes of the locations feature only.

Each video call can comprise four or six call streams. For a video call, total bandwidth represents the sum of the call audio bandwidth plus video bandwidth but does not include the call overhead.

The audio bandwidth value that is specified for a location includes overhead, whereas the video bandwidth value that is specified for a location does not include overhead. For a location, the bandwidth that is available for video calls represents the sum of the audio bandwidth and the video bandwidth. See the Video telephony, on page 543 chapter for more details.

Cisco Unified Communications Manager allows calls to complete over a link until sufficient bandwidth does not exist for a new call. At that point, any additional calls fail, and the calling party receives reorder tone.

When a link to a location experiences blockage, it may result from bandwidth leakage that has reduced the usable bandwidth for the location. You can resynchronize the bandwidth allotment to the maximum setting for the location without restarting the Cisco Unified Communications Manager server.

If you resynchronize the bandwidth for a location when calls are using the link, the bandwidth might be oversubscribed until all calls that are using the link disconnect. An oversubscribed link can cause audio and video quality to degrade. For this reason, resynchronize the location bandwidth during hours when the link has low traffic.

Media Termination Point (MTP) and transcoder represent exceptions to the bandwidth rules that are outlined in the preceding paragraph. Calls that are made through an MTP can complete even if they exceed the available bandwidth limit. Calls that are made through an MTP, however, cannot provide video.

In the United States and Canada, routing an emergency 911 call to a link that has no more available bandwidth can block the 911 call. For each location on your network, always route 911 calls to the local public switched telephone network (PSTN) through a local VoIP gateway.

See the “Regions” subtopic under the “Administration Considerations” topic of the “IP Video Telephony” chapter of the Cisco Unified Communications Solution Reference Network Design (SRND) for the current release, which provides recommendations as to how the video bandwidth should be set for regions and locations, so the video portion of video calls will succeed, and the video calls will not get rejected nor set up as audio-only calls.

**Location-based MLPP**

Cisco Unified Communications Manager supports MLPP on phones that run SCCP and TDM (PRI/CAS) trunks. Cisco Unified Communications Manager also supports MLPP on wide-area network (WAN) links. Location-based call admission control (CAC) manages WAN link bandwidth in Cisco Unified Communications Manager. Enhanced locations take into account the precedence level of calls and preempt calls of lower precedence when necessary to accommodate higher precedence calls.

Enhancing locations mean that, when a precedence call arrives and not enough bandwidth can be found to connect the call to the destination location, Cisco Unified Communications Manager finds the call or calls with the lowest precedence level and preempts the call(s) to make sufficient bandwidth available for a higher
precedence call. If the bandwidth requirement still cannot be satisfied after going through the preemption procedure, the newly placed call fails.

**Location-based call admission control over intercluster trunk**

When a call gets made across cluster through an intercluster trunk (ICT) and gets hairpinned back to the same location or site of the same cluster, although the media gets exchanged between two endpoints in the same site or location, the previous design of Cisco Unified Communications Manager location call admission control (CAC) deducted location bandwidth twice, once for the outbound call and again for the inbound call. The result did not correctly reflect the bandwidth consumption, which eventually caused denial of a new call to or from the site or location.

To resolve the bandwidth calculation problem, this feature enables Cisco Unified Communications Manager to pass location information, the primary key ID (PKID) of location record and location name, as a proprietary information element (IE) between the calling and called parties through an ICT, either in the H.323 protocol or SIP. Thus, either endpoint knows the true location information of the party/endpoint, not the location information of the ICT.

Cisco Unified Communications Manager previously identified Hub_None as the default location that has unlimited bandwidth, plus any user-created location to which the user can assign a device and for which the user can configure bandwidth.

A Cisco Unified Communications Manager location gets created specifically for the ICT for this type of application. This location, designated as the Phantom location, also has unlimited bandwidth. The locations server does not deduct bandwidth for a device that is assigned to the Phantom location. A device, such as the ICT, that is assigned to the Phantom location can use its own location or the true location of the connected device. Likewise, the outbound ICT can use its own location or the callee location, and the inbound ICT can use its own location or the caller location to deduct or adjust the bandwidth.

When the media connects, Cisco Unified Communications Manager adjusts the allocated location bandwidth according to the negotiated media codec. Cisco Unified Communications Manager can correctly readjust the location bandwidth on the basis of received callee location information for the outbound call. This enhancement helps the outbound call, which has reserved bandwidth during call setup time, to adjust the bandwidth back to 0 if the call gets hairpinned back to the same site or location.

Some supplementary services, such as transfer, can also hairpin the call back to the same site or location after the initial call setup process. Be aware that passing the location information of the final destination through the Notify signals (H.323) and re-INVITE signals (SIP) back to the calling cluster, so bandwidth can be adjusted to the right value, is also required.

Because location record PKID is uniquely defined within the Cisco Unified Communications Manager enterprise environment, Cisco Unified Communications Manager uses location record PKID to identify whether the call over ICT has looped back to the same cluster for the location-based CAC purpose. If other applications, like Cisco Voice Proxy (CVP), do not have access to the Cisco Unified Communications Manager database for location record PKID information, which comprises a string of characters and digits, applications may need to rely on the location name information that is getting passed around for the purpose of CAC. The same location name may exist for different locations with different location PKIDs in two different Cisco Unified Communications Manager clusters, which may cause confusion to the applications.

**Cisco Unified Communications Manager Administration Configuration Tips**

The Location Configuration window specifies the Phantom location as a location, besides the Hub_None location, that can get selected. Administrators cannot delete the Phantom location.
Administrators can create a default location for the Phantom location, similar to the Hub_None location. The Phantom location includes unlimited audio and video bandwidth value, and the administrator cannot modify the audio and video bandwidth values. The user can assign a location-pair RSVP policy between this location and other existing locations.

This feature does not entail any additional menu options or fields in Cisco Unified Communications Manager Administration. The Phantom value gets added for all entities that specify a location in the Location drop-down list box. You can find the Location field on the Device Pool Configuration, Annunciator Configuration, Music On Hold (MOH) Server Configuration, Conference Bridge Configuration, Voice Mail Port Configuration, Voice Mail Port Wizard Configuration, CTI Route Point Configuration, Gateway Configuration, Phone Configuration, Trunk Configuration, and Pilot Point Configuration windows.

Cisco Unified Communications Manager maintains the RSVP policy for the Phantom location during migration.

Tip
If the intercluster trunk or H.323 gateway gets configured in any other location besides the Phantom location, this feature does not work. In addition, if the intercluster trunk is connected to a third-party system that does not recognize and pass the Cisco-specific location information in the SIP or H.323 signals, this feature does not work.

Related Topics
SIP trunk, on page 453

Configure gatekeepers and trunks

A gatekeeper device, the Cisco Multimedia Conference Manager (MCM), provides call admission control for distributed call-processing systems. In a distributed system, each site contains its own call-processing capability.

Sometimes an anonymous H.323 device, a device that is not known to Cisco Unified Communications Manager, tries to initiate (send or receive) calls with Cisco Unified Communications Manager. This anonymous device could be a Cisco IOS product (such as a gateway) or any third-party H.323 device.

You can configure H.323 gateways either with gatekeeper control or locally as gateways.

Procedure

Step 1
Select Device > Trunk.

Step 2
Choose an option from the Trunk Type drop-down list box.

<table>
<thead>
<tr>
<th>Select...</th>
<th>To...</th>
</tr>
</thead>
<tbody>
<tr>
<td>H.225 Trunk (Gatekeeper Controlled)</td>
<td>Configure an anonymous H.323 device.</td>
</tr>
<tr>
<td>Intercluster Trunk (Gatekeeper Controlled)</td>
<td>Configure a remote endpoint.</td>
</tr>
<tr>
<td>Intercluster Trunk (Non-Gatekeeper Controlled)</td>
<td>Connect two Cisco Unified Communications Manager services in remote clusters.</td>
</tr>
</tbody>
</table>

Step 3
Configure the appropriate fields when the Trunk Configuration window displays.
Call admission control example

This illustration shows two sites, each with its own Cisco Unified Communications Manager, that an IP WAN link connects. A gatekeeper provides call admission control over the IP WAN link in this example.

Figure 6: Call admission control by using a gatekeeper in a distributed system

In addition to call admission control, gatekeepers can perform E.164 address resolution to route calls between sites. In this example, the extension range for one Cisco Unified Communications Manager specifies 1XXX and 2XXX for the other. Both register with the gatekeeper for call admission control. Each Cisco Unified Communications Manager incorporates an appropriate entry in its respective dial plan route pattern configuration that points the other Cisco Unified Communications Manager extension number range to the gatekeeper. In practice, when user 1001 dials user 2002, Cisco Unified Communications Manager 1XXX sends 2002 to the gatekeeper for address resolution. If the call satisfies the call admission control criteria, the gatekeeper returns the IP address of Cisco Unified Communications Manager 2XXX to Cisco Unified Communications Manager 1XXX. Using the IP address of Cisco Unified Communications Manager 2XXX, Cisco Unified Communications Manager 1XXX can then complete the call to directory number 2002.

If the IP WAN is not available in this scenario, the call cannot go through as dialed. To simplify the dial plan and also provide fallback to the PSTN, use 10-digit dialing (or adhere to the national dial plan). For example, under the North American Numbering Plan (NANP), a route pattern of XXXXXXXXXX would direct calls to the gatekeeper for address resolution. If the gatekeeper does not allow the call to go over the WAN, Cisco Unified Communications Manager can add the prefix 91 to the dialed digits to reroute the call through the PSTN.

See the Cisco Unified Communications Solution Reference Network Design (SRND) for more detailed information about gatekeeper configuration, dial plan considerations when a gatekeeper is used, and gatekeeper interaction with Cisco Unified Communications Manager.

Related Topics

Configure gatekeeper and gatekeeper-controlled trunk, on page 67
Configure gatekeeper and trunk on the router, on page 76
Components of gatekeeper call admission control

Gatekeeper call admission control provides great flexibility:

- Gatekeepers reduce configuration overhead by eliminating the need to configure a separate H.323 device for each remote Cisco Unified Communications Manager that is connected to the IP WAN.
- A gatekeeper can determine the IP addresses of devices that are registered with it, or you can enter the IP addresses explicitly.
- The gatekeeper supports the H.323 protocol and uses the H.225 protocol to make calls.
- The gatekeeper can perform basic call routing in addition to call admission control.

Configure gatekeeper and trunk on the router

Recommended platforms for the gatekeeper include Cisco 2600, 3600, 3700, or 7200 routers with Cisco IOS Release 12.1(3)T or higher. When configuring the gatekeeper function on one of these routers, you define a set of zones for call admission control. The unique name for each zone includes the IP address of each Cisco Unified Communications Manager that registers with that zone, the zone prefix (directory number range), and the bandwidth that is allocated for that zone.

Cisco Unified Communications Manager registers with a gatekeeper by using its IP address. You can specify the IP address in one of the following ways:

- Use the `gw-type-prefix` command on the gatekeeper to specify each Cisco Unified Communications Manager IP address explicitly.
- In the Technology Prefix field under Device > Trunk in Cisco Unified Communications Manager Administration, enter `1#*` and enter the command `gw-type-prefix 1#* default-technology` on the gatekeeper. When a Cisco Unified Communications Manager registers with the gatekeeper, it sends its IP address and the specified technology prefix to the gatekeeper. The gatekeeper then registers this Cisco Unified Communications Manager as a valid gatekeeper-controlled VoIP device.

You associate the Cisco Unified Communications Manager IP address with a particular zone by performing the following steps:

- Use the `zone local` command on the gatekeeper to define local zones. Enter the zone name in the Zone field.
- In the Zone field under Device > Trunk in Cisco Unified Communications Manager Administration, enter the zone name. When a Cisco Unified Communications Manager registers with the gatekeeper, it sends its IP address and the specified zone name to the gatekeeper. The gatekeeper then registers each Cisco Unified Communications Manager and associates it with the appropriate zone.

To specify the directory number range for a particular Cisco Unified Communications Manager, you use the zone prefix command to configure the range on the gatekeeper. For example, the following command specifies that the DN for zone LHR ranges from 3000 to 3999.

```
zone prefix LHR 3...
```

The maximum number of active calls that are allowed per zone depends on the codec that is used for each call and the bandwidth that is allocated for the zone. With Cisco Unified Communications Manager, G.711 calls request 128 kb/s, and G.723 and G.729 calls request 20 kb/s. Use regions in Cisco Unified Communications
Manager to specify the codec type and use the bandwidth total zone command on the gatekeeper to specify the available bandwidth. For example, the following command allocates 512 kb/s to the LHR zone.

```
bandwidth total zone LHR 512
```

With an allocation of 512 kb/s, the LHR zone in this example could support up to four G.711 calls at the same time.

**Related Topics**

Configure gatekeepers and trunks, on page 74

---

**Configure gatekeeper and trunk in Cisco Unified Communications Manager**

You can configure gatekeepers and trunks in Cisco Unified Communications Manager Administration to function in either of the following ways:

**Non-Gatekeeper-Controlled Trunks**

In this case, you explicitly configure a separate intercluster trunk for each remote device cluster that the local Cisco Unified Communications Manager can call over the IP WAN. You also configure the necessary route patterns and route groups to route calls to and from the various intercluster trunks. The intercluster trunks statically specify the IP addresses of the remote devices. To choose this method, use **Device > Trunk** and select **Inter-Cluster Trunk (Non-Gatekeeper Controlled)** in Cisco Unified Communications Manager Administration.

**Note**

For a local non-gatekeeper-controlled intercluster trunk, you must specify the IP addresses of all remote Cisco Unified Communications Manager nodes that belong to the device pool of the remote non-gatekeeper-controlled intercluster trunk.

**Gatekeeper-Controlled Trunks**

In this case, a single intercluster trunk suffices for communicating with all remote clusters. Similarly, you need a single H.225 trunk to communicate with any H.323 gatekeeper-controlled endpoints. You also configure route patterns or route groups to route the calls to and from the gatekeeper. In this configuration, the gatekeeper dynamically determines the appropriate IP address for the destination of each call to a remote device, and the local Cisco Unified Communications Manager uses that IP address to complete the call.

This configuration works well in large as well as smaller systems. For large systems where many clusters exist, this configuration helps to avoid configuring individual intercluster trunks between each cluster. To choose this method, use **Device > Trunk** and select **Inter-Cluster Trunk (Gatekeeper Controlled)** in Cisco Unified Communications Manager Administration.

If you configure gatekeeper-controlled trunks, Cisco Unified Communications Manager automatically creates a virtual trunk device. The IP address of this device changes dynamically to reflect the IP address of the remote device as determined by the gatekeeper. Use trunks when configuring the route patterns or route groups that route calls to and from a gatekeeper.
Resource Reservation Protocol

Resource Reservation Protocol (RSVP) specifies a resource-reservation, transport-level protocol for reserving resources in IP networks. RSVP provides an additional method to achieve call admission control (CAC) besides location-based CAC. Location-based CAC constitutes a point-to-point CAC mechanism that does not take into account topology changes nor multi-tiered topologies, whereas RSVP does take these into account.

- The following factors call for RSVP support as an alternative call admission control (CAC) mechanism in Cisco Unified Communications Manager:
  - Many customers request a full-mesh network topology for their video conferencing and video telephony environment to match their existing topology. If Cisco Unified Communications Manager does not support an RSVP-based CAC mechanism, a location-based CAC mechanism can still be leveraged as a viable solution.
  - The Quality of Service (QoS) baseline recommends that all VoIP and videoconferencing devices provide admission control by using RSVP.

For more information on call admission control (CAC), see the Call admission control, on page 65.

This section provides an overview of RSVP, describes RSVP configuration within Cisco Unified Communications Manager, discusses migration to RSVP, shows example RSVP interactions, and provides troubleshooting information.

- Configure RSVP, page 80
- RSVP overview, page 80
- RSVP agent and quality of service, page 83
- RSVP configuration, page 85
- Migrate to RSVP, page 93
- RSVP interactions, page 94
- Troubleshooting RSVP, page 100
Configure RSVP

Resource Reservation Protocol (RSVP) specifies a resource-reservation, transport-level protocol for reserving resources in IP networks. RSVP provides an additional method to achieve call admission control (CAC) besides location-based CAC. Location-based CAC constitutes a point-to-point CAC mechanism that does not take into account topology changes nor multi-tiered topologies, whereas RSVP does take these into account.

Procedure

Step 1 Configure the clusterwide default RSVP policy.
Step 2 Configure the RSVP policy for any location pair that requires a different RSVP policy from the clusterwide default RSVP policy.
Step 3 Configure other RSVP-related service parameters:
   - RSVP Retry
   - Midcall RSVP Error Handling
   - MLPP-to-RSVP Priority Mapping
   - TSpec
   - DSCP
   - Application ID
Step 4 Configure RSVP Agents for media devices.
Step 5 Configure end-to-end RSVP over SIP trunks.
Step 6 Enable RSVP for a call.

Related Topics
- RSVP configuration, on page 85
- RSVP for media devices, on page 91
- Use RSVP between clusters, on page 91
- Enable RSVP for a call, on page 92

RSVP overview

RSVP includes the following features:

- RSVP reservations get made for a particular session. A session comprises a flow that has a particular destination address, destination port, and a protocol identifier (TCP or UDP). RSVP reservations treat each session as one independent unit.
- RSVP messages travel along the same path as the media flow path.
- RSVP specifies a unidirectional protocol, so flows get reserved in only one direction.
• RSVP specifies a receiver-oriented protocol; as such, the receiver of the stream requests the reservation.
• RSVP supports both unicast and multicast environments.
• RSVP messages flow transparently through non-RSVProuters and switches.

Advantages of RSVP

The following factors make RSVP a more desirable solution than location-based call admission control (CAC) for providing quality of service (QoS):

• RSVP can handle complex topologies. Location-based CAC supports only hub-and-spoke or point-to-point topologies, such as simple Multiprotocol Label Switching (MPLS) any-to-any topologies. Locations cannot properly support multi-tiered topologies. Location-based CAC does not handle complex topologies, such as the following:
  ◦ Redundant links (A = B)
  ◦ More than three sites in a series (A - B - C - D)
  ◦ Multilevel hierarchies (hubs, regions, and subregions)
  ◦ Meshes

• RSVP exhibits network awareness, whereas location-based CAC cannot handle dynamic changes to bandwidth.

• IP videoconferencing not only requires significant bandwidth but also requires specialized service from the network with respect to latency and packet loss. RSVP enables network to accommodate such traffic without unduly degrading the performance of other applications in the network.

• RSVP supports Multilevel Precedence and Preemption (MLPP) inherently.

RSVP capabilities

The following capabilities get built on top of RSVP:

• RSVP supports all signaling protocols, including SIP, SCCP, MGCP, and H.323.
• RSVP works by enforcing a location-pair-based RSVP policy. You can enable and disable RSVP based on location pairs. This practice allows for migration.
• The setting of a systemwide service parameter determines RSVP policy for the system. Therefore, you can enable or disable RSVP throughout the system. Location-pair-based policies, however, override the systemwide policy.
• RSVP provides the following RSVP policy levels:
  ◦ No reservation (Continue using location-based CAC.)
  ◦ Mandatory
  ◦ Optional (video desired)
  ◦ Mandatory (video desired)
RSVP contains a retry reservation capability. This capability allows a call to gain or regain premium Quality of Service (QoS) even if the resources (bandwidth) are not currently available.

The RSVP Retry Timer controls the frequency of retry. The Mandatory RSVP Midcall Retry Counter and Mandatory RSVP mid call error handle option service parameters control the number of attempts to restore premium service by reserving the necessary resources if the initial RSVP policy specifies Mandatory.

RSVP integrates with Differentiated Services (DiffServ) QoS. The outcome of an RSVP reservation updates the Differentiated Services Code Point (DSCP) value.

The midcall failure policy that RSVP has means that this capability allows a user to determine what happens to the call if the call loses the bandwidth reservation in mid call. The following options exist:

- The call fails after N reservation retries.
- The call becomes a best-effort call.

RSVP supports bandwidth reservation for both audio and video streams.

RSVP provides application ID support.

RSVP supports Multilevel Precedence and Preemption (MLPP).

RSVP retains the reservation when a party gets put on hold. The reserved resource(s) can potentially get reused when the call resumes.

Shared-line devices that are located in the same location/region share the same reservation for incoming calls.

RSVP works with all Cisco Unified Communications Manager supplementary services and features to ensure that bandwidth reservation is correct after the service or feature is invoked. Examples of supported features include Call Transfer, Conference, and Call Forwarding.

RSVP supports Music on Hold (MOH) and annunciator features.

### RSVP-based MLPP

When RSVP is configured, MLPP functions as follows:

- Cisco Unified Communications Manager passes the precedence level of the MLPP call to the RSVP agent by means of SCCP Quality of Service (QoS) messages.
- Agents add priority information to RSVP requests.
- IOS routers can use this priority information to admit calls.
- If preemption occurs at the IOS router, the RSVP agent notifies Cisco Unified Communications Manager about the reservation failure due to preemption.
- Cisco Unified Communications Manager notifies the preempted calling party and called party of the preemption. Cisco Unified Communications Manager uses the existing MLPP functionality, which resembles the location-based call admission control (CAC) MLPP preemption mechanism.
- Preempted calls can either fail or continue with decreased QoS. Preempted calls receive the same treatment as midcall reservation failure.
Additional features

Cisco Unified Communications Manager supports the following interactions:

- RSVP agent supports Differentiated Services Control Point (DSCP) remarking. This capability mitigates the trust issues with desktop applications, such as Communicator and VTA.
- RSVP supports audio, video, and data pass-through. Video data pass-through allows video and data packets to flow through RSVP agent and media termination point devices. Video data pass-through also allows audio transcoding to work with video calls. Audio pass-through allows encrypted calls to flow through MTPs.

Pass-Through Conditions

The following conditions apply to both audio and video/data pass-through:

- All intermediate MTP devices support pass-through.
- No “MTP required” check box is checked for either endpoint.

The following additional audio pass-through condition applies:

- A matching audio cap exists between two endpoints after region filtering.

The following additional video pass-through condition applies:

- All intermediate MTP devices support multimedia. That is, MTP devices support multiple channels per call.

RSVP caveats

RSVP presents the following support limitations:

- Cisco Unified Communications Manager does not support RSVP interaction with endpoints that support RSVP natively.
- RSVP does not support the G. Clear Codec.

RSVP agent and quality of service

Cisco Unified Communications Manager uses an RSVP agent, which is an IOS-based RSVP proxy with an SCCP interface to support RSVP. Cisco Unified Communications Manager communicates with the RSVP agent through a set of SCCP messages. The RSVP agent registers with Cisco Unified Communications Manager as either a media termination point or a transcoder device.

Note

RSVP does not conflict with Automated Alternate Routing (AAR), which continues to function if AAR is configured. See the Automated Alternate Routing, on page 144 for details.
Each endpoint requires an RSVP agent. The agent pair (one agent for endpoint A, another agent for endpoint B) signals RSVP on behalf of the endpoints that Cisco Unified Communications Manager controls.

**RSVP agent example**

This figure illustrates an example of a Cisco Unified Communications Manager network with RSVP that is configured through an RSVP agent.

*Figure 7: Cisco Unified Communications Manager network configured with RSVP Agent*

---

**RSVP agent allocation**

Cisco Unified Communications Manager allocates the RSVP agent resource in the same manner that it allocates media termination point and transcoder resources. You configure a Media Resource Group List (MRGL) that includes the RSVP agent and assign the MRGL to the device or the device pool that associates with the device. RSVP reservation fails if the same RSVP agent is assigned to both endpoints that are making a call.

**RSVP agent interaction with location-based CAC**

Cisco recommends that you do not activate both location-based Call Admission Control (CAC) and RSVP at the same time, except during the migration period from location-based CAC to RSVP.

If location bandwidth is not set to unlimited (infinite bandwidth) in the location, Cisco Unified Communications Manager performs location-based CAC before performing RSVP. If location-based CAC fails, the call fails, and Cisco Unified Communications Manager does not invoke RSVP.

If location bandwidth is set to unlimited (infinite bandwidth) in the location, Cisco Unified Communications Manager invokes RSVP based on RSVP policy for the location pair that is associated with the calling and the called parties.
RSVP configuration

RSVP configuration comprises configuration of various service parameters and other components. The sections that follow describe the various service parameters and other configuration that is needed to configure RSVP.

Tip

Before you configure RSVP, see the Configure RSVP, on page 80.

Related Topics

Configure RSVP, on page 80

Configure clusterwide default RSVP policy

To configure the clusterwide RSVP policy, configure the following clusterwide (System - RSVP) service parameter for the Cisco CallManager service:

Procedure

Step 1 In Cisco Unified Communications Manager Administration, choose the System > Service Parameters menu option.

Step 2 In the Service Parameter Configuration window, choose a server and choose the Cisco CallManager service.

Step 3 In the Clusterwide Parameters (System - RSVP) section, configure the Default interlocation RSVP Policy service parameter.

You can set this service parameter to the following values:

- No Reservation-No RSVP reservations get made between any two locations.
- Optional (Video Desired)-A call can proceed as a best-effort, audio-only call if failure to obtain reservations for both audio and video streams occurs. RSVP agent continues to attempt RSVP reservation for audio and informs Cisco Unified Communications Manager if reservation succeeds.
- Mandatory-Cisco Unified Communications Manager does not ring the terminating device until RSVP reservation succeeds for the audio stream and, if the call is a video call, for the video stream as well.
- Mandatory (Video Desired)-A video call can proceed as an audio-only call if a reservation for the audio stream succeeds but a reservation for the video stream does not succeed.

Configure location-pair RSVP policy

Use the Location Configuration window to configure the RSVP policy for a given location pair. The RSVP policy that is configured for a location pair overrides the default interlocation RSVP policy that you configure in the Service Parameter Configuration window.

To configure the RSVP policy for a pair of locations, configure the RSVP Setting field for the location pair:
Procedure

Step 1  In Cisco Unified Communications Manager Administration, choose the System > Location menu option.

Step 2  Find one location of the location pair and select this location.

Step 3  To modify the RSVP policy between the selected location and another location, select the other location in the location pair.

Step 4  In the RSVP Setting drop-down list box, choose an RSVP policy for this location pair.

You can set this field to the following values:

- Use System Default—The RSVP policy for the location pair matches the clusterwide RSVP policy. See the Configure clusterwide default RSVP policy, on page 85 for details.
- No Reservation—No RSVP reservations get made between any two locations.
- Video Desired (Optional)—A call can proceed as a best-effort, audio-only call if failure to obtain reservations for both audio and video streams occurs. The RSVP agent continues to attempt RSVP reservation for audio and informs Cisco Unified Communications Manager if reservation succeeds.
- Video Desired—A video call can proceed as an audio-only call if a reservation for the audio stream succeeds but the reservation for the video stream does not succeed.

Configure RSVP retry

Use the following clusterwide (System - RSVP) service parameters to configure the frequency and number of RSVP retries:

- RSVP Retry Timer
- Mandatory RSVP Midcall Retry Counter

To locate and configure these service parameters, follow these steps:

Procedure

Step 1  In Cisco Unified Communications Manager Administration, choose the System > Service Parameters menu option.

Step 2  In the Service Parameter Configuration window, choose a server and choose the Cisco CallManager service.

Step 3  In the Clusterwide Parameters (System - RSVP) section, configure the specified service parameters.

You can set these service parameters to the following values:

- RSVP Retry Timer—Specify the RSVP retry timer value in seconds. If you set this parameter to 0, you disable RSVP retry on the system.
- Mandatory RSVP Midcall Retry Counter—Specify the midcall RSVP retry counter when the RSVP policy specifies Mandatory and midcall error handling option is set to “call fails following retry counter exceeds.”
Configure midcall RSVP error handling

Use the following clusterwide (System - RSVP) service parameter to configure midcall RSVP error handling:

- Mandatory RSVP mid call error handle option

To locate and configure this service parameter, follow these steps:

**Procedure**

**Step 1**
In Cisco Unified Communications Manager Administration, choose the **System > Service Parameters** menu option.

**Step 2**
In the Service Parameter Configuration window, choose a server and choose the Cisco CallManager service.

**Step 3**
In the Clusterwide Parameters (System - RSVP) section, configure the specified service parameter.

You can set the Mandatory RSVP mid call error handle option service parameter to the following values:

- Call becomes best effort-If RSVP fails during a call, the call becomes a best-effort call. If retry is enabled, RSVP retry attempts begin simultaneously.
- Call fails following retry counter exceeded-If RSVP fails during a call, the call fails after N retries of RSVP, where the Mandatory RSVP Mid-call Retry Counter service parameter specifies N.

Configure MLPP-to-RSVP priority mapping

Use the following clusterwide (System - RSVP) service parameters to configure the mapping from a caller MLPP precedence level to RSVP priority:

- MLPP EXECUTIVE OVERRIDE To RSVP Priority Mapping
- MLPP FLASH OVERRIDE To RSVP Priority Mapping
- MLPP FLASH To RSVP Priority Mapping
- MLPP IMMEDIATE To RSVP Priority Mapping
- MLPP PL PRIORITY To RSVP Priority Mapping
- MLPP PL ROUTINE To RSVP Priority Mapping

To locate and configure these service parameters, follow these steps:
Procedure

**Step 1** In Cisco Unified Communications Manager Administration, choose the **System > Service Parameters** menu option.

**Step 2** In the Service Parameter Configuration window, choose a server and choose the Cisco CallManager service.

**Step 3** In the Clusterwide Parameters (System - RSVP) section, configure the specified service parameters. These service parameters function as follows:

- Cisco Unified Communications Manager maps the caller precedence level to RSVP priority when initiating an RSVP reservation based on the following configuration: the higher the service parameter value, the higher the priority.
- The IOS router preempts the call based on RSVP priority.
- The RSVP agent must notify Cisco Unified Communications Manager about the reason for an RSVP reservation failure, including the cause for preemption.
- Cisco Unified Communications Manager uses the existing MLPP mechanism to notify the preempted calling and called parties about the preemption.

**TSpec**

The TSpec object describes the traffic that the sender generates. The TSpec gets transported through the network to all intermediary routers and to the destination endpoint. The intermediate routers do not change this object and the object gets delivered unchanged to the ultimate receiver(s).

The TSpec object comprises the following elements:

- averageBitRate (kb/s)
- burstSize (bytes)
- peakRate (kb/s)

**Audio TSpec**

For audio flows, the TSpec calculations specify the following measurements:

- burstSize (bytes)-This value gets calculated as the size of the packet times the number of packets in a burst. For audio flows, the burst usually specifies 1 to 2.
- peakRate (bytes)-The peakRate, in bytes, refers to the maximum bytes/second that the endpoint transmits at any given time. If the burst is small, as is the case in audio streams, the peakRate can be calculated as 1.1 (or 1.2) times the tokenRate.

To avoid adjusting the bandwidth reservation upward when the call gets answered, Cisco Unified Communications Manager reserves the maximum bandwidth for each region codec at call setup time. Cisco Unified Communications Manager then modifies or adjusts the bandwidth based on the media capability of the connected parties when the call gets answered.
**Example Audio TSpec Calculations**

See the following examples of bandwidth calculations for different region codecs for call setup.

G.711: 8 sample/frame; for 10-ms packet: \( 80 + 40 \) (header) = 120 \( \times \) 100 (packets/sec) = 12000 \( \times \) 8 = 96 kb/s; 
\[
\text{TSpec.mAverageBitRate} = \text{bwPlusHeader} = 96 \text{ kb/s};
\]
\[
\text{TSpec.mPeakRate} = \text{TSpec.mAverageBitRate} \times (1.2) = 115; 
\]
\[
\text{TSpec.mBurstSize} = \text{PacketSize} \times 2 = 120 \times 2 = 240; 
\]

G.729: 10 ms/frame; 8 kb/s; Default is 20 ms; 0 and 10 are possible. For 10-ms packet: \( 10 + 40 = 50 \) \( \times \) 100 = 5000 \( \times \) 8 = 40 kb/s 
\[
\text{kb/s: (packet_size_in_ms+40)*8000/packet_size_in_ms} 
\]

The TSpec of the G.711 codec specifies the following calculations:

\[
\text{Tspec.mAverageBitRate} = \text{bwPlusHeader} = 96 \text{ kb/s};
\]
\[
\text{Tspec.mPeakRate} = \text{Tspec.mAverageBitRate} \times (1.2) = 115; 
\]
\[
\text{Tspec.mBurstSize} = \text{PacketSize} \times 2 = 120 \times 2 = 240; 
\]

**Video TSpec**

For video streams, the packet length does not depend on codecs. Individual implementations provide the basis for packet length. Also, the packet sizes do not remain uniform across all packets. Estimating the number of packets per second therefore proves difficult.

Assume that the maximum packet size for a video stream specifies 1000 bytes.

The RSVP Video Tspec Burst Size Factor service parameter in the Clusterwide Parameters (System - RSVP) section of the service parameters for the Cisco CallManager service allows you to configure the video stream burst size. The default value for this service parameter specifies 5.

The following elements comprise the video Tspec:

- burstSize (bytes)-Burst size factor (5) * max packet size (1000)
- peakRate (bytes)-This element refers to the maximum bytes/second that the endpoint transmits at any given time. If the burst is small, as is the case with audio streams, you can calculate the peakRate as 1.1 (or 1.2) times the tokenRate.

Cisco Unified Communications Manager attempts to use the bandwidth for the entire video call to reserve bandwidth for the video stream first: 384 kb + overhead.

Example: \( 384 + 27 = 410 \) kb/s 

If insufficient bandwidth exists for the entire video call, Cisco Unified Communications Manager next attempts to reserve the following amount of bandwidth: (video call bandwidth - audio stream codec) + overhead).

Example: \( (384 - 64) + 22 = 342 \) kb/s 

The Tspec for the 384 kb codec specifies the following calculations:

\[
\text{Tspec.mAverageBitRate} = \text{bwPlusHeader} = 410 \text{ kb/s};
\]
\[
\text{Tspec.mPeakRate} = \text{Tspec.mAverageBitRate} = 410;\text{Tspec.mBurstSize} = 1000 \times 5 = 5000;
\]

**DSCP**

If the RSVP reservation fails, Cisco Unified Communications Manager instructs the RSVP agent or endpoint devices (in case a failure to allocate an RSVP agent occurs) to change media Differentiated Services Control.
Point (DSCP) marking to best effort. Otherwise, an excess of EF-marked media packets can degrade quality of service (QoS) even for flows that have a reservation.

Cisco Unified Communications Manager uses the clusterwide (System - QoS) DSCP for Audio Calls When RSVP Fails service parameter or the DSCP for Video Calls When RSVP Fails service parameter to determine the DSCP values for this instruction when RSVP fails for the call.

**Application ID**

An application ID specifies an RSVP object that can be inserted in a policy element in an RSVP message. RFC 2872 describes this object. This policy object serves to identify the application and associates the application with the RSVP reservation request, thus allowing routers along the path to make appropriate decisions based on the application information.

The following clusterwide (System - RSVP) system parameters allow configuration of application IDs:

- RSVP Audio Application ID
- RSVP Video Application ID

When a voice call is made between locations with an RSVP policy, the resulting reservations for the audio stream get tagged with the RSVP Audio Application ID. When a video call is made between locations with an RSVP policy, the resulting reservations for the audio stream and the video stream get tagged with the RSVP Video Application ID.

If a call changes from audio to video, the following happens:

- The existing audio reservation gets released from the audio pool.
- The audio bandwidth reservation is re-attempted in the video pool with optional policy.
- The Application ID for the audio stream gets changed to RSVP Video, and the new video stream gets tagged with the RSVP Video Application ID.

If a video call changes to an audio call, the following happens:

- Both existing audio and video reservations are released from the video pool.
- The audio bandwidth reservation is re-attempted in the audio pool with optional policy.
- The Application ID for the audio stream gets changed to RSVP Audio.

**Note**

In an end-to-end RSVP environment, when the audio bandwidth reservation is re-attempted in either the audio or video pool, both clusters try to release the audio bandwidth from the existing pool and re-attempt the audio reservation in the new pool. This can cause a race condition that might take up to a re-try cycle to complete before the audio bandwidth reservation in the new pool happens.

By using this call admission control model, you can reserve a certain amount of bandwidth for voice calls and allow them to use the entire available bandwidth in the priority queue, thus ensuring that all the available bandwidth can be used for voice calls if no video calls are in progress. If enough available bandwidth exists in the priority queue, calls can optionally be enabled for video. You can set limits on how much bandwidth the video-enabled calls can consume, but if voice calls are consuming all the available bandwidth, it might not be possible to place a video call at all.
**RSVP for media devices**

Because conference bridges, music on hold servers, and annunciators do not specify Media Resource Group List (MRGL) configuration, you make RSVP resources available for these devices by associating these devices with a device pool that has an associated RSVP agent. The MRGL that is associated with the device pool gets used to allocate RSVP resources for these types of media devices.

**Related Topics**

Configure RSVP, on page 80

---

**Use RSVP between clusters**

RSVP supports reservations between end points in separate clusters by using two different configurations: local and end-to-end.

**Local RSVP**

Local RSVP does not support reservations between two RSVP agents that are located in different clusters. It uses two RSVP agents per cluster, and does not use RSVP across the trunk that connects the clusters. This is the default configuration.

Consider the following scenario:
endpoint A - agentA - agentICT1 - ICT1 - ICT2 - agentICT2 - agentB - endpoint B

where A specifies an endpoint in cluster 1, B specifies an endpoint in cluster 2, ICT1 and ICT2 specify the intercluster trunks within clusters 1 and 2, and the RSVP Agents associate with the respective devices.

In this scenario, Cisco Unified Communications Manager 1 controls the reservation between agentA and agentICT1, and Cisco Unified Communications Manager 2 controls the reservation between agentB and agentICT2.

As an alternative, you can use Cisco Unified Border Element (formerly Cisco Multiservice IP-to-IP) gateways. See the Configure gatekeepers and trunks, on page 74 for more information.

**End-to-End RSVP**

End-to-end RSVP configuration is available if the clusters are connected by a SIP trunk. End-to-end RSVP uses RSVP on the entire connection between the end points, and uses only one RSVP agent per cluster.

Consider the following scenario:
endpoint A - agentA - ICT1 - ICT2 - agentB - endpoint B

where A specifies an endpoint in cluster 1, B specifies an endpoint in cluster 2, ICT1 and ICT2 specify the intercluster trunks within clusters 1 and 2, and the RSVP Agents associate with the respective end points.

In this scenario, Cisco Unified Communications Manager establishes an end-to-end RSVP connection between agentA and agentB.

**Configuring End-to-End RSVP Over a SIP Trunk**

RSVP configuration on a SIP trunk is determined by the SIP profile that is applied to the trunk. To enable end-to-end RSVP on a SIP trunk, configure the trunk’s SIP profile as follows:

- From the RSVP Over SIP drop-down list, choose E2E.
- Set the Fall back to local RSVP field to your preference.
- From the SIP Rel1XX Options drop-down list, choose an option other than Disabled.
Enable RSVP for a call

To enable RSVP for a call, follow these steps:

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Assign the calling device and the called device to different locations.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Either configure default interlocation policy to any setting other than “No Reservation” or use the Location Configuration window to configure the RSVP setting for the two locations to anything other than “No Reservation.”</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Assign a Media Resource Group List (MRGL) that includes an RSVP agent resource to both endpoint devices. Use either the configuration window for the devices or the Device Pool Configuration window.</td>
</tr>
</tbody>
</table>

Special configuration with RSVP

In an RSVP session, special configuration applies if all the following conditions exist:

- One endpoint device, such as Cisco IP Interactive Voice Response (IP IVR), was configured to support only the G.711 codec.
- RSVP was configured for the call.
- The interregion codec specifies G.729 between the calling RSVP agent and the called RSVP agent.

When the call is made, to achieve successful allocation and reservation of RSVP agent resources and bandwidth, the administrator must configure the media termination point (MTP)/RSVP agent with the G.729 codec in addition to the pass-through codec. This configuration allows insertion of a transcoder between the RSVP agent of the called side and the called device at the time of media connection. When codecs match, codec pass-through takes place; if codecs do not match, the call cannot continue without a transcoder.

If configuration of the G.729 codec in the agent does not take place, the call will fail because Cisco Unified Communications Manager will not invoke a transcoder that is needed for the RSVP call.

The situation arises if either of the following conditions apply: the interregion codec gets used between calling and called agents or between two endpoints that specify G.729. Two options exist to enable successful routing of this call:

- Use RSVP agent for IVR as a transcoder. In this case, the interregion codec between the transcoder/RSVP agent and IVR needs to specify the G.711 codec.
- Use software MTP as RSVP Agents and insert a transcoder between IVR and the RSVP agent for IVR. In this case, ensure the software MTP is configured with the G.729 codec in addition to the pass-through codec.
Keep in mind that the RSVP agent that has transcoding capability cannot perform G.729-to-G.729 transcoding. If you use a transcoder as an RSVP agent, you either must use the pass-through codec or configure the transcoder, so one of the codecs that is used on both sides of the transcoder specifies G.711.

**Migrate to RSVP**

Migration from location-based call admission control (CAC) to RSVP requires that you take some special circumstances into consideration. During the RSVP deployment time period, devices in some locations will probably have RSVP agent that is configured while others do not have RSVP agent that is configured. When a call takes place from a location that has RSVP agent to another location that does not have RSVP agent, Cisco Unified Communications Manager will manage the quality of service (QoS) of the call by using both location-based CAC and RSVP. The first part of the call, from the location that has RSVP agent to the hub/central site that has RSVP, uses the RSVP mechanism. The second part of the call, from the hub/central site to the location that does not have RSVP, gets managed through location-based CAC. If either mechanism fails to allocate bandwidth, the call fails.

**Procedure**

| Step 1 | Install RSVP agent A at Location 1. |
| Step 2 | Install RSVP agent B at Location 0 (hub). |
| Step 3 | Add agent A to the Media Resource Group List of all endpoints at Location 1. |
| Step 4 | Add agent B to the Media Resource Group List of all endpoints not at Location 1, including devices at the hub and at all other locations. |
| Step 5 | Configure RSVP policy from Location 1 to all other locations to be Mandatory (or some other policy, if desired). |
| Step 6 | Change the location CAC bandwidth limit for Location 1 to unlimited. |

This illustration shows a location configuration to which the migration process applies.

*Figure 8: Migrating the First Spoke of a Location Configuration*

After you perform the preceding configuration steps, the following bandwidth applies to the locations:
After you perform the preceding configuration steps, the following RSVP policies apply:

### Table 7: RSVP policies

<table>
<thead>
<tr>
<th>Location Pair</th>
<th>RSVP Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 1</td>
<td>None</td>
</tr>
<tr>
<td>1 Not 1</td>
<td>Mandatory</td>
</tr>
<tr>
<td>Not 1 Not 1</td>
<td>None</td>
</tr>
</tbody>
</table>

After you take the preceding configuration steps, the following call admission control (CAC) takes place:

- Calls within locations 0, 2, 3, and 4 use the same CAC as before.
- Calls within location 1 are not subject to CAC.
- Calls between location 0 and location 1 use RSVP CAC.
- Calls between location 1 and locations 2, 3, or 4 have RSVP on the 0-to-1 link and location-based CAC on the 0-to-2, 0-to-3, or 0-to-4 link. If either mechanism fails, the call fails.

### RSVP interactions

The following sections provide examples of RSVP interaction with various Cisco Unified Communications Manager features and services.

### RSVP and IPv6

RSVP does not support IPv6. RSVP calls support IPv4. If RSVP is required for the call and any device in the call is configured for or uses an IPv6 address, Cisco Unified Communications Manager rejects the call, and the caller receives a busy tone. For more information on IPv6, see [RSVP and MLPP](RSVP and MLPP) on page 98.
RSVP and shared-line calls

This illustration shows the RSVP interaction during the alerting phase of a shared-line call.

Figure 9: RSVP During a Shared-Line Call (Alerting Phase)

The example shows the following configuration during the alerting phase of the shared-line call:

- Phones B1 (in location 2), B2 (in location 3), and B3 and B4 (both in location 4) share the DN 2000.
- The RSVP agent in location 1 has a single reservation. The reservation has multiple destinations, one to each RSVP agent in the other locations (2, 3, and 4).
- RSVP agent in location 4 has one allocated reservation. Phones B3 and B4 share this reservation.

Phones B3 and B4, which share the DN 2000, use a single RSVP agent.

This illustration shows the RSVP interaction after a shared-line call gets answered.

Figure 10: RSVP During a Shared-Line Call (Call Answered Phase)
After phone B2 (in location 3) answers the shared-line call, the RSVP reservation between location 1 and location 2, as well as the reservation between location 1 and location 4, get torn down. Only the RSVP reservation between location 1 and location 3 remains established.

**RSVP and music on hold**

This illustration shows a call that invokes Music On Hold. Phones A and B are in a call when phone B puts phone A on hold. In this example, the MOH server resides in the same location as phone A.

*Figure 11: Phone B Puts Phone A on Hold, MOH Server in Same Location as Phone A*

RSVP preserves the reservation between phone A and phone B while phone A is on hold and receiving Music On Hold. After the call between phone A and phone B resumes, the reserved resource gets reused. Because phone A and the MOH server that provides its music on hold are in the same location, no need exists for RSVP reservation between phone A and the MOH server.

This illustration shows a call that invokes Music On Hold. Phones A and B are in a call when phone B puts phone A on hold. In the illustration, the MOH server resides in the same location as phone B.

*Figure 12: Phone B Puts Phone A on Hold, MOH Server in Same Location as Phone B*

This example shows a phone call between phone A and phone B, with the music on hold server in the same location as phone B. If phone B puts phone A on hold, so phone A receives music on hold, the reservation that was used to connect phone A and phone B gets reused for the music on hold session. No additional reservation gets created.
This illustration shows a call that invokes music on hold. Phones A and B are in a call when phone B puts phone A on hold. In the illustration, the MOH server occupies a different location from both phone A and phone B. (Phone A, phone B, and the music on hold server each reside in a different location.)

Figure 13: Phone B Puts Phone A on Hold, MOH Server in a Third Location

If phone B puts phone A on hold, so phone A receives music on hold, RSVP agent preserves the reservation that was used to connect phone A and phone B. Another RSVP agent creates a new reservation between phone A and the MOH server.

**RSVP and call transfer**

This illustration shows the initial scenario, where phone A is in a call with phone B.

Figure 14: Call from Phone A to Phone B with RSVP Agent Connection

In the illustration, phone A, DN 1000, location 1, calls phone B, DN 2000, location 2. RSVP agent establishes a reservation for the call. Phone B presses the Transfer button and dials DN 3000. Phone C, DN 3000, location 4, answers the call.
This illustration shows the RSVP connections as phone B transfers the call to phone C.

*Figure 15: Phone B Initiates Transfer of Call from Phone A to Phone C*

When phone B initiates transfer of the call from phone A to phone C in this configuration, the RSVP agent preserves the reservation between phone A and phone B. An RSVP agent creates a new RSVP reservation between phone A and the MOH server. An RSVP agent creates a new reservation between phone B and phone C.

This illustration shows the scenario after the transfer completes.

*Figure 16: Call Transfer Completes, and Phone A and Phone C Get Connected*

After phone B completes the transfer, a new RSVP reservation gets created between phone A and phone C. The RSVP reservations between phone A and the MOH server, phone A and phone B, and phone B and phone C, all get torn down.

**RSVP and MLPP**

The following sections discuss various RSVP-based MLPP scenarios.

**Scenario 1: A lower priority call gets preempted during congestion.**

Initial call RSVP Policy: Mandatory
Midcall RSVP Policy: Call fails. No retries
Other configuration details: RSVP bandwidth equals 100 kb/s. Each call takes 80 kb/s; therefore, only one call can obtain a reservation successfully.

1 Start a Priority call.
   The call succeeds.

2 Start a Routine call.
   The call fails to initialize due to the Mandatory setting.

3 Start a Flash call.
   The call succeeds because the Priority call gets preempted.

Scenario 2: A video call proceeds as an audio-only call if sufficient bandwidth does not exist.
Initial call RSVP Policy: Mandatory with video desired
Midcall RSVP Policy: Best effort
Other configuration details: RSVP bandwidth equals 100 kb/s. Each audio call takes 80 kb/s; therefore, only one call can obtain a reservation successfully.

1 Start a Priority audio call.
   The call succeeds.

2 Start a Flash video call.
   The call starts as audio only because insufficient bandwidth exists for a video call. The quality of the Priority call decreases.

Scenario 3: A lower priority call continues during congestion with no premium QoS.
Initial call RSVP Policy: Optional
Midcall RSVP Policy: Best effort
Other configuration details: RSVP bandwidth equals 100 kb/s. Each audio calls takes 80 kb/s; therefore, only one call can obtain a reservation successfully.

1 Start a Priority call.
   The call succeeds.

2 Start a Routine call.
   The call succeeds, but no premium QoS is available. (The call uses a different DSCP.)

3 Start a Flash call.
   The call succeeds. The QoS for the Priority call decreases.

4 End (hang up) the Flash call.
   The Priority call recovers the RSVP reservation, and QoS increases.
Troubleshooting RSVP

For information about troubleshooting end-to-end RSVP, see the Troubleshooting end-to-end RSVP, on page 102.

RSVP provides the performance monitoring (PerfMon) counters, Call Detail Records (CDRs), alarms, and trace information to assist with troubleshooting RSVP.

Performance monitoring counters

The following Cisco Unified Communications Manager RSVP admission control performance monitoring counters exist:

- RSVP AudioReservationErrorCounts
- RSVP MandatoryConnectionsInProgress
- RSVP OptionalConnectionsInProgress
- RSVP TotalCallsFailed
- RSVP VideoCallsFailed
- RSVP VideoReservationErrorCounts

These location-based and node-based performance monitoring counters do not synchronize across nodes. To troubleshoot RSVP agent resources, the following RSVP performance monitoring counters exist:

- OutOfResources
- ResourceActive
- ResourceAvailable
- ResourceTotal

See the Cisco Unified Real Time Monitoring Tool Administration Guide for descriptions of the performance monitoring counters and instructions on how to view performance monitoring counters.

Call detail records

The Cisco Unified Communications Manager Quality of Service (QoS) RSVP agent feature adds the following Call Detail Record (CDR) fields:

- origRSVPAudioStat-Status of RSVP audio reservation from originator to terminator
- destRSVPAudioStat-Status of RSVP audio reservation from terminator to originator
- origRSVPVideoStat-Status of RSVP video reservation from originator to terminator
- destRSVPVideoStat-Status of RSVP video reservation from terminator to originator

These fields reflect the status of RSVP bandwidth reservation per audio or video stream. The following values apply for the Cisco Unified Communications Manager RSVP CDR status fields:
• 0-Indicates RSVP NO RESERVATION condition, which is the default value.
• 1-Indicates RSVP RESERVATION FAILURE condition at call setup or feature invocation.
• 2-Indicates RSVP RESERVATION SUCCESS condition at call setup or feature invocation.
• 3-Indicates RSVP RESERVATION NO RESOURCE (RSVP agent) condition at call setup or feature invocation.
• 4-Indicates RSVP MID_CALL FAILURE_PREEMPTED condition (preempted after call setup).
• 5-Indicates RSVP MID_CALL FAILURE_LOST_BANDWIDTH condition (includes all midcall failure except MLPP preemption).

The Cisco Unified Communications Manager RSVP CDR status field value gets concatenated, and the most recent 32 status values get retained for the call.

**Example**

A call establishes with the Optional RSVP policy, and the initial RSVP reservation succeeds. The call subsequently loses its bandwidth reservation and regains the bandwidth reservation after retrying. This sequence repeats several times during the call, and the call ends with a successful RSVP reservation. In this case, the CDR shows the following string as the Cisco Unified Communications Manager RSVP reservation status for that particular stream:

```
```

See the Cisco Unified Communications Manager CDR Analysis and Reporting Administration Guide for additional information.

**Alarms**

The RsvpNoMoreResourcesAvailable alarm gets generated when no RSVP agent resource is available.

The following Cisco Unified Communications Manager alarm catalog defines this alarm:

```
/vob/ccm/Common/XML/AlarmCatalog/Communications Manager.xml.
```

**Trace information**

RSVP generates several SDL and SDI traces for the Cisco CallManager service upon RSVP reservation failure. The user sees the RSVP error codes in both the Cisco Unified Communications Manager SDL and SDI trace files.

The RSVP agent can send the following RSVP Reservation error codes:

• `QOS_CAUSE_RESERVATION_TIMEOUT=0`,
• `QOS_CAUSE_PATH_FAIL`,
• `QOS_CAUSE_RESV_FAIL`,
• `QOS_CAUSE_LISTEN_FAIL`,
• `QOS_CAUSE_ResourceUnavailable`,
• `QOS_CAUSE_LISTEN_TIMEOUT`,
• `QOS_CAUSE_RESV_RETRIES_FAIL`,
Troubleshooting end-to-end RSVP

This section provides troubleshooting information for end-to-end RSVP. For more information about end-to-end RSVP, see the Use RSVP between clusters, on page 91.

Table 8: Troubleshooting End-to-End RSVP

<table>
<thead>
<tr>
<th>Problem</th>
<th>Recommended Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>After a tandem/remote transfer, the final call is no longer an end-to-end RSVP call.</td>
<td>In the transferring node, make sure that the RSVP policy is activated between locations to which the inbound and outbound SIP trunk is assigned.</td>
</tr>
<tr>
<td>When the call is put on hold, there is no end-to-end RSVP between the MOH server and a held party.</td>
<td>In the holding cluster, make sure that the MOH’s device pool has a MRGL that has the RSVP agents assigned. Also make sure RSVP policy is activated between locations to which the MOH server and SIP trunk are assigned.</td>
</tr>
<tr>
<td>When a device in campus (Hub_none location) makes or receives a call, there is no end-to-end RSVP.</td>
<td>Make sure that RSVP policy is activated between the Hub_none location and location to which the SIP trunk is assigned.</td>
</tr>
<tr>
<td>When a conference call gets invoked, there is no end-to-end RSVP between the conference bridge and remote conference participants.</td>
<td>In the cluster that invoked the conference call, make sure that the conference bridge’s device pool has a MRGL that has the RSVP agents assigned. Also make sure that RSVP policy is activated between locations to which the conference bridge and SIP trunks are assigned.</td>
</tr>
<tr>
<td>When a call gets blind transferred to a remote system, there is no end-to-end RSVP between the announciator and the calling phone.</td>
<td>In the transferring cluster, make sure that the announciator’s device pool has a MRGL that has the RSVP agents assigned. Also make sure RSVP policy is activated between locations to which the announciator and SIP trunks are assigned.</td>
</tr>
<tr>
<td>A basic end-to-end RSVP call fails.</td>
<td>Make sure that the RSVP policy has been activated between endpoint and trunk on both the clusters, and that the SIP profile for the inbound and outbound SIP trunk is configured to support end-to-end RSVP on both clusters.</td>
</tr>
<tr>
<td>Problem</td>
<td>Recommended Action</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>End-to-end RSVP reservation fails.</td>
<td>A possible cause is that the same router is being used as the calling and called RSVP agents, and that router is not running the latest IOS version, which supports loopback on RSVP reservation. Make sure that the router is running the latest IOS version.</td>
</tr>
</tbody>
</table>
Cisco **TFTP**

This chapter provides information about the Cisco TFTP service which builds and serves files that are consistent with the Trivial File Transfer Protocol (TFTP). Cisco TFTP builds configuration files and serves embedded component executables, ringer files, and device configuration files.

A configuration file contains a prioritized list of Cisco Unified Communications Managers for a device (phones that are running SCCP and phones that are running SIP and gateways), the TCP ports on which the device connects to those Cisco Unified Communications Managers, and an executable load identifier. Configuration files for selected devices contain locale information and URLs for the phone buttons: messages, directories, services, and information. Configuration files for gateways contain all their configuration information.

You can find configuration files in a .cnf, a .cnf.xml, or an .xml format, depending on the device type and your TFTP service parameter settings. When you set the Build CNF Files service parameter to Build All, the TFTP server builds both .cnf.xml and .cnf format configuration files for all devices. When you set this service parameter to Build None, the TFTP server builds only .cnf.xml files for all devices. When this parameter is set to Build Selective, which is the default value, the TFTP server builds .cnf.xml files for all devices and, in addition, builds .cnf files only for a select list of device types that are provided in Table 11-1:

*Table 9: Devices with Build Selective BuildCNFType*

<table>
<thead>
<tr>
<th>Device Type</th>
<th>Device Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>MODEL_30SPP</td>
<td>Cisco 30 SP+</td>
</tr>
<tr>
<td>MODEL_12SPP</td>
<td>Cisco 12 SP+</td>
</tr>
<tr>
<td>MODEL_12SP</td>
<td>Cisco 12 SP</td>
</tr>
<tr>
<td>MODEL_12S</td>
<td>Cisco 12 S</td>
</tr>
<tr>
<td>MODEL_30VIP</td>
<td>Cisco 30 VIP or DPA</td>
</tr>
<tr>
<td>MODEL_IP_CONFERENCE_PHONE</td>
<td>Cisco 7935</td>
</tr>
<tr>
<td>MODEL_SCCP_PHONE</td>
<td>SCCP Phone</td>
</tr>
<tr>
<td>MODEL_VEGA</td>
<td>Analog Access</td>
</tr>
</tbody>
</table>
Configure TFTP

The Cisco TFTP service builds and serves files that are consistent with the Trivial File Transfer Protocol (TFTP). Cisco TFTP builds configuration files and serves embedded component executables, ringer files, and device configuration files.

A configuration file contains a prioritized list of Cisco Unified Communications Managers for a device (phones that are running SCCP and phones that are running SIP and gateways), the TCP ports on which the device connects to those Cisco Unified Communications Managers, and an executable load identifier. Configuration files for selected devices contain locale information and URLs for the phone buttons: messages, directories, services, and information. Configuration files for gateways contain all their configuration information.

Configure the Cisco TFTP service with the following steps.

Procedure

Step 1 Activate and start the Cisco TFTP service on the appropriate server.
Step 2 Configure the appropriate service parameters, including the Alternate File Location parameters, if appropriate.
Step 3 If you change a non-configuration file such as a load file or RingList.xml, start and stop the Cisco TFTP service.

Note You must upload files to the TFTP directory from Cisco Unified Communications Operating System Administration.
TFTP process overview for devices that run SCCP

The TFTP server can handle simultaneous requests for configuration files. This section describes the request process.

When a device boots, it queries a DHCP server for its network configuration information. The DHCP server responds with an IP address for the device, a subnet mask, a default gateway, a Domain Name System (DNS) server address, and a TFTP server name or address. (Some devices, such as the Cisco Unified IP Phone 7960, support up to two TFTP servers. If the primary TFTP server is not reached, such devices attempt to reach the fallback TFTP server.)

Note
If DHCP is not enabled on a device, you must assign it an IP address and configure the TFTP server locally on the device.

The device requests a configuration file from the TFTP server. The TFTP server searches three internal caches, the disk, and then alternate Cisco file servers (if specified) for the configuration file. If the TFTP server finds the configuration file, it sends it to the device. If the configuration file provides Cisco Unified Communications Manager names, the device resolves the name by using DNS and opens a connection to the Cisco Unified Communications Manager. If the device does not receive an IP address or name, it uses the TFTP server name or IP address for setting up its registration connection.

If the TFTP server cannot find the configuration file, it sends a “file not found” message to the device.

Note
If the TFTP server returns a “file not found” message to the device, a “request not found” TFTP counter increments. In nonsecure clusters, this behavior does not represent an error because the CTL file does not exist on a Cisco Unified Communications Manager in nonsecure mode.

Devices that are requesting a configuration file while the TFTP server is rebuilding configuration files or while processing the maximum number of requests receive a message from the TFTP server, which causes the device to request the configuration file later. The Maximum Serving Count service parameter, which can be configured, specifies 200 as the maximum number of requests.

For a more detailed description of how devices boot, see the Devices that use DHCP and Cisco TFTP, on page 110.

Configure TFTP for Cisco Unified IP phones that run SIP

Unlike phones that are running SCCP, phones that are running SIP get all their configurations from the TFTP server. From initial startup, the phone that is running SIP contacts the configured TFTP server (either manually configured or configured through the DHCP server) to get the configuration files; it then registers itself to its configured Cisco Unified Communications Manager.

When the configuration of the phone that is running SIP gets changed, the Cisco Unified Communications Manager database notifies the TFTP server to rebuild all the configuration files or to rebuild selectively. The TFTP server retrieves information from the Cisco Unified Communications Manager database and converts it into the proper output format, according to the device type, and saves the output in TFTP cache. When the TFTP server gets a request, it searches either the cache or Alternate File Server locations disk to serve the requested configuration file or default files.
The TFTP support for phones that are running SIP builds and serves different formats of SIP configuration files from the Cisco Unified Communications Manager database for the following Cisco Unified IP Phones:

- Cisco Unified IP Phone 7970/71, 7961, 7941, 7911 (These phones share the same SIP configuration file format.)
- Cisco Unified IP Phone 7960, 7940 (These phones share the same SIP configuration file format.)
- Cisco Unified IP Phone 7905, 7912
- SIP dial plans on the preceding phones
- Softkey templates on the preceding phones

The TFTP server generates the following files from the Cisco Unified Communications Manager database for configuration of phones that are running SIP:

- Systemwide default configuration files and per-device configuration files.
- List of systemwide dial plans for Cisco Unified IP Phones 7970/71, 7960/61, 7940/41, and 7911.
- List of systemwide softkey template files.

Table 11-3 lists the configuration files that get generated based on the type of phone that is running SIP.

<table>
<thead>
<tr>
<th>SIP Configuration File Type</th>
<th>Model 7970/71, 7961, 7941, 7911</th>
<th>Model 7960/40</th>
<th>Model 7905</th>
<th>Model 7912</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP IP Phone</td>
<td>SEP&lt;mac&gt;.cnf.xml</td>
<td>SIP&lt;mac&gt;.cnf</td>
<td>&lt;dialplan&gt;.xml</td>
<td>gk&lt;mac&gt;</td>
</tr>
<tr>
<td>Dial Plan</td>
<td>DR&lt;dialplan&gt;.xml</td>
<td>Parameter in ld&lt;mac&gt;</td>
<td>Parameter in gk&lt;mac&gt;</td>
<td></td>
</tr>
<tr>
<td>Softkey Template</td>
<td>SK&lt;softkey_template&gt;.xml</td>
<td>Not configurable</td>
<td>Not configurable</td>
<td>Not configurable</td>
</tr>
</tbody>
</table>

The system derives filenames from the MAC Address and Description fields in the Phone Configuration window of Cisco Unified Communications Manager Administration and the devicename field in the Cisco Unified Communications Manager database. The MAC address uniquely identifies the phone.

**Configuration Sequence for a Phone That Is Running SIP**

The configuration sequence for a phone that is running SIP performs the following steps:
**Procedure**

**Step 1** The administrator makes a change to the phone that is running SIP (for example, by using Phone Configuration, SIP Profile Configuration, or SIP Phone Security Profile Configuration in Cisco Unified Communications Manager Administration) and clicks Save.

**Step 2** The Cisco Unified Communications Manager database sends a change notification to the TFTP server and to Cisco Unified Communications Manager. The TFTP server then rebuilds all the configuration files for the selected phone. The configuration file name and format depend on the device type and protocol (see Table 11-3).

**Step 3** The administrator presses the reset/restart button to reset/restart the phones that are affected by the changes.

**Step 4** Upon notification (automatically, by the administrator, or by the user), Cisco Unified Communications Manager notifies the phone to get the configuration files again.

**Step 5** The phone that is running SIP requests the configuration files from the TFTP server, and the server sends the requested files to the phone.

**Step 6** After getting the necessary configuration files, the phone registers its configured lines with Cisco Unified Communications Manager.

### Dial Plan Configuration Sequence for a Phone That Is Running SIP

The dial plan configuration sequence for a phone that is running SIP performs the following steps:

**Procedure**

**Step 1** The administrator configures the SIP dial plan and associates the dial plan with the phone that is running SIP.

**Step 2** The Cisco Unified Communications Manager database sends a change notification to the TFTP server, which triggers the TFTP server to build a new set of files for the phone that is running SIP.

**Step 3** The TFTP server rebuilds the Dial Plan configuration file and/or the configuration file for the phone that is running SIP.

**Step 4** When all the updates to the dial rules have been made to the Cisco Unified Communications Manager database, the administrator clicks the Reset or Restart button to apply the change to the phone.

### Softkey Template Configuration Sequence for a Phone That Is Running SIP

The softkey template configuration sequence for a phone that is running SIP performs the following steps:
Procedure

Step 1 The administrator configures the SIP softkey template and associates the softkey template with the phone that is running SIP.

Step 2 The Cisco Unified Communications Manager database sends a change notification to the TFTP server, which triggers the TFTP server to build a new set of files for the phone that is running SIP.

Step 3 The TFTP server rebuilds the softkey template configuration file and/or the configuration file for the phone that is running SIP.

Step 4 When all the updates to the softkeys have been made to the Cisco Unified Communications Manager database, the administrator presses the Reset or Restart button to apply the change to the phone.

Interaction with Cisco Extension Mobility

When a user logs into a device by using Cisco Extension Mobility, the Cisco Unified Communications Manager database notifies the TFTP server to rebuild the SEP<mac>.cnf.xml file to include the new dial plan filenames that are defined for the lines on the device profile.

Serviceability Counters

The TFTP server provides counters in Cisco Unified Serviceability for troubleshooting purposes.

Tip

If the TFTP server returns a “file not found” message to the device, a “request not found” TFTP counter increments. In nonsecure clusters, this behavior does not represent an error because the CTL file does not exist on a Cisco Unified Communications Manager in nonsecure mode.

Devices that use DHCP and Cisco TFTP

Cisco telephony devices require IP addresses that are assigned manually or by using DHCP. Devices also require access to a TFTP server that contains device loads and device configuration files.

Obtaining an IP Address

If DHCP is enabled on a device, DHCP automatically assigns IP addresses to the device when you connect it to the network. The DHCP server directs the device to a TFTP server (or to a second TFTP server, if available for the device). For example, you can connect multiple Cisco Unified IP Phones anywhere on the IP network, and DHCP automatically assigns IP addresses to them and provides them with the path to the appropriate TFTP server.

If DHCP is not enabled on a device, you must assign it an IP address and configure the TFTP server locally on the device.

The default DHCP setting varies depending on the device:

- Cisco Unified IP Phones stay DHCP-enabled by default. If you are not using DHCP, you need to disable DHCP on the phone and manually assign it an IP address.
- DHCP remains always enabled for Cisco Access Analog and Cisco Access Digital Gateways.
- For Cisco Catalyst 6000 8 Port Voice T1/E1 and Services Modules, the Network Management Processor (NMP) on the Cisco Catalyst 6000 may or may not have DHCP enabled. If DHCP is not enabled, you will need to configure the IP address through the Cisco CATOS command-line interface on the Cisco Catalyst 6000.

**Requesting the Configuration File**

After a device obtains an IP address, it requests a configuration file from the TFTP server.

If a device has been manually added into the Cisco Unified Communications Manager database, the device accesses a configuration file that corresponds to its device name. If a phone is not manually configured and auto-registration is enabled, the phone requests a default configuration file from the TFTP server and starts the auto-registration procedure with Cisco Unified Communications Manager.

---

**Note**

Phones represent the only device type that can auto-register and that have default configuration files. You must manually add all other devices to the Cisco Unified Communications Manager database.

If a phone has an XML-compatible load, it requests a .cnf.xml format configuration file; otherwise, it requests a .cnf file.

---

**Note**

When you set the Build CNF File service parameter to Build All, the TFTP server builds both .cnf.xml and .cnf format configuration files for all devices. When you set this service parameter to Build None, the TFTP server builds only .cnf.xml files for all devices. When this parameter is set to Build Selective, which is the default value, the TFTP server builds .cnf.xml files for all devices and, in addition, builds .cnf files only for a select list of devices that do not support .cnf.xml. Table 11-1 provides a list of these devices.

**Contacting Cisco Unified Communications Manager**

After obtaining the configuration file from the TFTP server, a device attempts to make a TCP connection to the highest priority Cisco Unified Communications Manager in the list that is specified in the configuration file. If the device was manually added to the database, Cisco Unified Communications Manager identifies the device. If auto-registration is enabled in Cisco Unified Communications Manager, phones that were not manually added to the database attempt to auto-register in the Cisco Unified Communications Manager database.

Cisco Unified Communications Manager informs devices that are using .cnf format configuration files of their load ID. Devices that are using .xml format configuration files receive the load ID in the configuration file. If the device load ID differs from the load ID that is currently executing on the device, the device requests the load that is associated with the new load ID from the TFTP server and resets itself. For more information on device loads, see the Device support, on page 119.

A phone gets the Ring Tones list after it performs its booting process, when the user wants to modify the Default Phone Ring setting, and when the user loads new ring tones.
TFTP server access for devices that use IPv4

You can enable the IP phones and gateways to discover the TFTP server IP address in one or more of the following ways, depending on the device type:

• Gateways and phones can use DHCP custom option 150.
  Cisco recommends this method. With this method, you configure the TFTP server IP address as the option value.

• Gateways and phones can use DHCP option 066.
  You may configure either the host name or IP address of the TFTP server as the option value.

• Gateways and phones can query Cisco CM1.
  Ensure the Domain Name System (DNS) can resolve this name to the IP address of the TFTP server. Cisco does not recommend this option because it does not scale.

• You can configure phones with the IP address of the TFTP server. If DHCP is enabled on the phone, you can still configure an alternate TFTP server IP address locally on the phone that will override the TFTP address that was obtained through DHCP.

• Gateways and phones also accept the DHCP Optional Server Name (sname) parameter.

• The phone or gateway can use the value of Next-Server in the boot processes (siaddr).

Devices save the TFTP server address in nonvolatile memory. If one of the preceding methods was available at least once, but is not currently available, the device uses the address that is saved in memory.

You can configure the TFTP service on the first node or a subsequent node, but usually you should configure it on the first node. For small systems, the TFTP server can coexist with a Cisco Unified Communications Manager on the same server.

TFTP server access for devices that use IPv6

Tip

This section assumes that the phone uses IPv6. If you have some phones that use IPv4 and some phones that use IPv6 in your network, Cisco recommends that you use DHCP custom option 150 for IPv4 and the TFTP Server Addresses sub-option type 1, a Cisco vendor-specific information option, for IPv6.

In an IPv6 network, the DHCPv6 server uses the Cisco vendor-specific DHCPv6 information options in the DHCPv6 response message to pass the TFTP IPv6 address to the device. If the device obtains an IPv6 address and sends a request to the TFTP server while the TFTP server is using IPv4 to process requests, the TFTP server does not receive the request because the TFTP server is not listening for the request on the IPv6 stack. In this case, the device cannot register with Cisco Unified Communications Manager.

You can enable the IP phones to discover the TFTP server IP address in one or more of the following ways, depending on the device type:

• Phones can use the TFTP Server Addresses sub-option type 1, which is a Cisco vendor-specific information option. Consider this option equivalent to Option 150.

  Cisco recommends this method. With this method, you configure the TFTP server IP address as the option value.
• Phones can use the TFTP Service sub-option type 2, which is another Cisco vendor-specific information option. Be aware that this option is equivalent to Option 66.

• You can configure phones with the IP address of the TFTP server. If DHCP is enabled on the phone, you can still configure on the phone an alternate TFTP server IP address that overrides the TFTP address that was obtained through DHCP.

Devices save the TFTP server address in nonvolatile memory. If one of the preceding methods was available at least once, but is not currently available, the device uses the address that is saved in memory.

You can configure the TFTP service on the first node or a subsequent node, but usually you should configure it on the first node. For small systems, the TFTP server can coexist with a Cisco Unified Communications Manager on the same server.

---

**Note**

If your Cisco Unified Communications Manager server supports IPv6, dual-stack devices can access a TFTP server by using IPv4 or IPv6 addresses.

---

**Note**

When a phone with SBD load, tries to register with a Cisco Unified Communications Manager which does not have SBD support, via a Proxy TFTP which supports SBD, the phone will be in a loop and will never register.

---

**Tip**

For more information on IPv6 and TFTP, see Device support, on page 119.

---

### Identify the TFTP server for devices

The following sections describe how gateways and Cisco Unified IP Phones identify the TFTP server.

#### Gateways

When gateways receive conflicting or confusing information from the DHCP server, they have an order of precedence that they use for selecting the address of the TFTP server. The basis for the order of precedence depends on the method that is used to specify the TFTP server (method 1 in the following list has the highest precedence).

1. Catalyst 6000 gateway uses a locally configured TFTP server address. This address overrides any TFTP address that the DHCP server sends.

2. The gateway queries the DNS name CiscoCM1, and it is resolved. The gateway always tries to resolve the DNS name CiscoCM1. If this name is resolved, it overrides all information that the DHCP server sends.

   You do not need to name the TFTP server CiscoCM1, but you must enter a DNS CName record to associate CiscoCM1 with the address or name of the TFTP server.

3. The gateway uses the value of Next-Server in the boot processes. The address of the TFTP server traditionally uses this DHCP configuration parameter. When BOOTP servers are configured, this field typically serves as the address of the TFTP server.
This information gets returned in the siaddr (server IP address) field of the DHCP header. Use this option, if available, because some DHCP servers will place their own IP address in this field when it is not configured.

4 The gateway that uses IPv4 uses the site-specific option 150. This option resolves the issue in which some servers do not allow the Next-Server configuration parameter. Some servers allow access to the Next-Server parameter only when IP addresses are statically assigned.

5 The gateway uses the Optional Server Name parameter. This DHCP configuration parameter designates the host name of a TFTP server. Currently, you can configure only a host name in this parameter; do not use a dotted decimal IP address.

6 The gateway that uses IPv4 uses the 066 option, which is the name of the boot server. Option 066 normally replaces the name (server name) field when option overloading occurs. This name field can contain a host name or a dotted decimal IP address. Do not use the 066 option with the 150 option. The device prefers the IP address over the name that is given by the 066 option if they are sent together. If both a dotted decimal IP address and a 150 option are sent, order of preference depends on the order in which they appear in the option list. The device chooses the last item in the option list because option 066 and option 150 remain mutually exclusive.

Cisco Unified IP Phones

Similar to gateways, Cisco Unified IP Phones 7971, 7970, 7961, 7941, 7931, 7911, 7906, 7960, and 7940 (that are using release 8.0(4) firmware and later) also have an order of precedence that they use for selecting the address of the TFTP server when they receive conflicting or confusing information from the DHCP server. The method that is used to specify the TFTP server (method 1 in the following list has the highest precedence) provides basis for the order of precedence.

1 Cisco Unified IP Phones use a manually configured alternate TFTP option, which is under the Settings Menu on the phone. When the alternate TFTP option is set to Yes locally on IP phones, both TFTP Server 1 and TFTP Server 2 address values override any TFTP addresses that the DHCP server sent.

2 Cisco Unified IP Phones use the option 150 value as the TFTP server IP address when Alternate TFTP option is set to No. You can assign only IP addresses as Option 150 values. A maximum of two IP addresses get used, and only the first two IP addresses that the DHCP server provides get accepted.

3 Cisco Unified IP Phones that use 066 option, which could be either a name (option 66 = DNS name) or dotted-decimal IP address (option 66 = dotted-decimal IP address) of the TFTP server. Be aware that the name may resolve to more than one address. Option 066 normally replaces the name (server name) field when option overloading occurs. This name field can contain a DNS name or a dotted decimal IP address. You cannot use multiple entries as part of this option values.

4 Cisco Unified IP Phones use the value of Next-Server IP Address in the boot-up processes as its TFTP server IP address. This DHCP configuration parameter traditionally gives the address of the TFTP server. Be aware that the name may resolve to more than one address. When you configure BOOTP servers, this field typically gets referred to as the address of the TFTP server. The siaddr (server IP address) field of the DHCP header returns this information.

5 Cisco Unified IP Phones use the Optional Server Name parameter name as the TFTP server name. This DHCP configuration parameter represents the DNS name of a TFTP server. Currently you can configure only a DNS name in this parameter; do not use a dotted decimal IP address.

Cisco recommends that you use DHCP custom option 150 for gateways and phones that use IPv4. With this method, the TFTP server IP address gets configured as the option 150 value. Phones only support two IP addresses for Option 150 values as TFTP Server 1 and TFTP Server 2 entries.
Be aware that option 66 is defined to be a string type, option 150 is defined as an array of 32-bit IP address(es), and both TFTP Server 1 and TFTP Server 2 are 32 bit IP addresses.

Configure a redundant TFTP server

You must have one TFTP server that is configured in a cluster; however, you may want to configure a redundant TFTP server. If a device (phone or gateway) gets no response from the first TFTP server, it tries to connect to the second TFTP server. Configure the second TFTP server in option 150 for IPv4 or the TFTP Server Addresses sub-option type 1 for IPv6 in the DHCP scope.

If the TFTP servers that are in the middle of rebuilding all configuration files return a delay message to the requesting device, the device does not attempt to use the second TFTP server; instead, it waits and retries the first TFTP server from which it received the message.

Alternate Cisco file servers

You can specify alternate Cisco file servers if you have multiple clusters, if you want to configure only one server for many DHCP scopes, or if you want to have one DHCP scope. You can configure alternate servers under Remote Cluster Service Configuration window (Advanced Settings > Cluster view). You can configure upto 3 alternate servers for a single cluster.

Ensure that the IP addresses of the alternate servers belong to the same cluster for which you are configuring the alternate servers.

For more information on configuring alternate TFTP servers, see

Cisco Unified Communications Manager supports both IPv4 and IPv6 addresses and hostnames that resolve to IPv4 and IPv6 addresses for alternate TFTP servers. The Enable IPv6 enterprise parameter does not affect serving files to off-cluster TFTP servers. If the TFTP server supports a dual IPv4/IPv6 stack, you can configure both an IPv4 and an IPv6 entry for an Alternate server and the system accesses the servers in the order that is configured.

You can configure the remote cluster information for the Primary TFTP server through Remote Cluster Service Configuration window (Advanced Features > Cluster View). Under each cluster you can configure the IP address of the TFTP server.

For more information on configuring remote clusters, see

The primary TFTP server serves configuration files from these servers for phones and devices in the external clusters. To avoid creating a loop, ensure that the TFTP servers on the external clusters do not point to each other.
Centralized TFTP in a multiple cluster environment

Centralized TFTP supports multiple Cisco Unified Communications Manager clusters within one regional, or site-specific environment, such as a large campus. Centralized TFTP allows devices (phones and gateways) to be moved, such as from one building to another, without requiring the administrator to reconfigure the device's IP settings (for example, DHCP, VLAN/DHCP).

Another example would be when several T1s terminate at the same demarcation point, but the T1s are to be distributed to several clusters, the administrator needs only to configure the T1s in the appropriate clusters and have the DHCP scope point the TFTP requests to the Master TFTP Server. The Centralized TFTP solution will provide the appropriate cluster-specific information to the individual T1s.

Centralized TFTP also supports multiple clusters that are running different operating systems. Devices that are registered and configured in any cluster can be directed to use a single TFTP server (the Master TFTP Server) that then serves cluster-specific files to those devices.

Master TFTP server

Each cluster must have at least one TFTP server. The primary function of the TFTP server is to build endpoint configuration files and to serve all files (such as configuration, security, firmware) to the endpoints.

In the Centralized TFTP environment, the Master TFTP Server represents a name that is applied to a single TFTP server, which gets designated to serve all files including security, firmware, and configuration files from all of the Cisco Unified Communications Manager clusters. Make this designation by simply directing all requests at the Master TFTP Server, either by hard-coding or by DHCP configuration at the endpoints.

Cisco strongly recommends that the Master TFTP Server belong to the cluster that has the most devices configured. In general, the system assumes that this configuration will provide the greatest chance for files to be found in the TFTP server cache and, therefore, will reduce the number of off-cluster searches.

Send files to the master TFTP server

When an off-cluster TFTP server receives a request from the Master TFTP Server, it searches for the file and, if found, sends the requested file back to the Master TFTP Server by using HTTP. The Master TFTP Server then uses TFTP to send the requested file to the device that originally requested the file. Should the off-cluster TFTP server not have the requested file, it will respond to the Master TFTP Server with File Not Found (HTTP Error 404). The Master TFTP Server continues the process with the next off-cluster TFTP server until either the file is located or no remaining options exist.

When the off-cluster server is busy, it sends HTTP Error 503 to the Master TFTP Server, so it should try the request again later. This message will also get sent to the endpoint device that made the original request.

Centralized TFTP with secure clusters

All off-cluster servers that are operating in mixed mode must add the Master TFTP Server or Master TFTP Server IP address to the off-clusters CTL file. (Without this updated CTL file, phones that register to a cluster where security is enabled and that attempt to download their config files will fail.) After the CTL file is updated, reboot the servers, so they can participate in the secure multicluster centralized TFTP network.

To update the CTL file for the TFTP servers, download the CTL Client plug-in by using Application > Install Plugins from Cisco Unified Communications Manager Administration.
Configure centralized TFTP

The following list comprises tips to remember when you are configuring a centralized TFTP environment:

- Only the master TFTP server gets configured with the remote clusters.

- If an Off-cluster belongs to Unified CM version 8.5 or earlier, ensure all off-cluster TFTP servers do not have Alternate Cisco File Server values configured. See “Service Parameter Configuration” in the Cisco Unified Communications Manager Administration Guide for information on how to configure the TFTP service.

- If you do not want Master TFTP server to be searched in a remote cluster, uncheck the ‘Enable’ check box for TFTP service in Remote Cluster Configuration window (Advanced Features > Cluster View).

- In general, Cisco does not recommend enabling auto-registration on Centralized TFTP Server. If auto-registration is enabled and any of the alternate file server is down, phones provisioned on this alternate file server will get auto-registered to Centralized TFTP server. Therefore, you should disable auto-registration if it is not already disabled or delete the accidentally registered phone after making sure that the cluster to which it belongs is up and running.

- For centralized TFTP configurations, ensure that the master TFTP server exists in the cluster that runs the highest version of Cisco Unified Communications Manager; for example, if you are using a centralized TFTP server between a compatible Cisco Unified CallManager 8.x cluster and a Cisco Unified Communications Manager 6.x cluster, ensure that your master TFTP server exists in the Cisco Unified Communications Manager 8.x cluster. If the master TFTP server exists in the cluster that runs the lower version of Cisco Unified Communications Manager, phones use locale files from the lower version of Cisco Unified Communications Manager, which can cause issues with the phone; for example, the phone displays Undefined or ??? for the Do Not Disturb feature instead of displaying that DND is active. These errors display on the phone because the locale files that are served to the phones from the master cluster do not include the localized phrases.

Customize and modify configuration files

You can add customized files (for example, ring tones, callback tones, phone backgrounds). If two TFTP servers exist in the cluster, ensure that the customized files are placed on both TFTP servers.
Device support

This chapter provides general information about how Cisco Unified Communications Manager interacts with Cisco Unified Communications devices in your network.

- Supported devices, page 119
- Device configuration files, page 120
- Device firmware loads, page 120
- Device pools, page 121
- Call preservation, page 121

Supported devices

The Cisco Unified Communications Manager supports many types of devices, including those in the following list:

- Cisco Unified IP Phones
- Analog gateway ports
- T1 gateway
- E1 gateway
- Transcoding resource
- Software Media Termination Point (MTP)
- Annunciator
- Conference resource (hardware)
- Conference resource (software)
- CTI port (TAPI and JTAPI)
- Cisco IP Softphone
- Messaging (voice mail)
- Intercluster trunk
Device configuration files

The Cisco Trivial File Transfer Protocol (Cisco TFTP) builds configuration files from information that is found in the Cisco Unified Communications Manager database.

The device-specific configuration files use the name format SEP, SAA, SDA, CFB, VGC, or MTP + MAC address:

- **SEP** - Selsius Ethernet Phone (Cisco IP Phone 12 SP+, Cisco IP Phone 30 VIP, Cisco Unified IP Phone 7902, Cisco Unified IP Phone 7905, Cisco Unified IP Phone 7906, Cisco Unified IP Phone 7910, Cisco Unified IP Phone 7911, Cisco Unified IP Phone 7912, Cisco Unified IP Phone 7920, Cisco Unified IP Phone 7921, Cisco Unified IP Phone 7931, Cisco Unified IP Phone 7935, Cisco Unified IP Phone 7936, Cisco Unified IP Phone 7940, Cisco Unified IP Phone 7941, Cisco Unified IP Phone 7960, Cisco Unified IP Phone 7961, Cisco Unified IP Phone 7970, and Cisco Unified IP Phone 7971)
- **SAA** - Selsius Analog Access (Cisco Catalyst 6000 24 Port FXS Analog Interface Module)
- **SDA** - Selsius Digital Access (Cisco Catalyst 6000 8 Port Voice E1/T1)
- **VGC** - Cisco VG248 Analog Phone Gateway (Cisco VG248 ports and units appear as distinct devices in the same Cisco Unified Communications Manager. All 48 device ports register within the same Cisco Unified Communications Manager as device type “Cisco VGC Phone.”)
- **MTP** - Media Termination Point

Configuration files also contain a list of Cisco Unified Communications Managers in priority order. Network addresses comprise either the fully qualified domain name, for example, “cm1.cisco.com,” or dotted IP address “172.116.21.12” plus a TCP port. See the Cisco TFTP, on page 105 for more information.

When a device needs to get its configuration file, the device sends a TFTP request for the device-specific configuration filename.

**Note**

You can specify button URLs in device configuration for Cisco Unified IP Phone 7970, 7960, and 7940. If the URL is blank, Cisco Unified Communications Manager uses the enterprise values.

Device firmware loads

Loads comprise files that contain updated firmware for devices. Four types of firmware loads exist: phone loads, gateway loads, MTP loads, and conference bridge loads. During installation or upgrade, Cisco Unified Communications Manager provides the latest loads; however, you can also receive a load between releases that can contain patches or other information that is important to the devices that use loads, such as phones or gateways.

The /usr/local/cm/tftp subdirectory stores these load files as *_.bin, _.zup, or _.sbin files; for example, D501A022.bin. During installation or upgrade, this location stores the latest loads. You must copy new loads that you receive between releases to this location for the system to access them.
To view the most current information on load descriptions for each device type, choose **Device > Device Settings > Device Defaults** and click the ? button.

### Update device loads

You can apply a new load to a single device before applying it as a systemwide default. This method can prove useful for testing purposes. Remember, however, that only the device that you have updated with the new load will use that load. All other devices of that type use the old load until you update the systemwide defaults for that device with the new load.

### Device pools

Device pools scale and simplify the distribution of Cisco Unified Communications Manager redundancy groups. Device pools allow you to assign the same configuration to a group of devices; for example, you can assign the device pool to phones, gateways, trunks, or CTI route points. In general, device pools allow you to configure common parameters that need to be applied to a device; for example, Cisco Unified Communications Manager Group, region, SRST reference, and so on. For phones, you may need to configure the device pool, the common phone profile, and the common device configuration, which work similarly to device pools (that is, they allow you to apply the same configuration to a group of phones). Be aware that some configuration settings in the device pool may not apply to all device types that use device pools; for example, the incoming called party settings apply only to H.323 trunks and gateways.

**Tip**

Optional calling search space can prevent rogue installations of IP phones on your network. For example, rogue phones that are plugged into the network autoregister in a device pool that has a calling search space that is restricted only to the Cisco Unified Communications Manager administrator. This search space can have a Primary Line Automatic Ringdown that is assigned to it, so, when the user goes off hook, the call immediately connects to security or the Cisco Unified Communications Manager administrator.

Typically, the following scenario applies with respect to configuring device pools. The deployment model drives the exact model of clustering and device pools that are used:

- **Region requirements for single-site cluster:** This scenario does not require use of regions because all calls use the G.711 codec for calls.
- **Total device pools** = Number of sites x regions.
  - Total device pools = Regions x Cisco Unified Communications Manager redundancy groups.

### Call preservation

The call preservation feature of Cisco Unified Communications Manager ensures that an active call does not get interrupted when a Cisco Unified Communications Manager fails or when communication fails between the device and the Cisco Unified Communications Manager that set up the call.

Cisco Unified Communications Manager supports full call preservation for an extended set of Cisco Unified Communications devices. This support includes call preservation between Cisco Unified IP Phones, Media Gateway Control Protocol (MGCP) gateways that support Foreign Exchange Office (FXO) (non-loop-start...
trunks) and Foreign Exchange Station (FXS) interfaces, and, to a lesser extent, conference bridge, MTP, and transcoding resource devices.

Enable H.323 call preservation by setting the advanced service parameter, Allow Peer to Preserve H.323 Calls, to True.

The following devices and applications support call preservation. If both parties connect through one of the following devices, Cisco Unified Communications Manager maintains call preservation:

- Cisco Unified IP Phones
- Software conference bridge
- Software MTP
- Hardware conference bridge (Cisco Catalyst 6000 8 Port Voice E1/T1 and Services Module, Cisco Catalyst 4000 Access Gateway Module)
- Transcoder (Cisco Catalyst 6000 8 Port Voice E1/T1 and Services Module, Cisco Catalyst 4000 Access Gateway Module)
- Non-IOS MGCP gateways (Catalyst 6000 24 Port FXS Analog Interface Module, Cisco DT24+, Cisco DE30+, Cisco VG200)
- Cisco IOS H.323 gateways (such as Cisco 2800 series, Cisco 3800 series)
- Cisco IOS MGCP Gateways (Cisco VG200, Catalyst 4000 Access Gateway Module, Cisco 2620, Cisco 3620, Cisco 3640, Cisco 3660, Cisco 3810)
- Cisco VG248 Analog Phone Gateway

The following devices and applications do not support call preservation:

- Annunciator
- H.323 endpoints such as NetMeeting or third-party H.323 endpoints
- CTI applications
- TAPI applications
- JTAPI applications

**Call preservation scenarios**

Table 9-1 lists and describes how call preservation is handled in various scenarios.
Table 10: Call Preservation Scenarios

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Call Preservation Handling</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Unified Communications Manager fails.</td>
<td>A Cisco Unified Communications Manager failure causes the call-processing function for all calls that were set up through the failed Cisco Unified Communications Manager to be lost. Cisco Unified Communications Manager maintains affected active calls until the end user hangs up or until the devices can determine that the media connection has been released. Users cannot invoke any call-processing features for calls that are maintained as a result of this failure.</td>
</tr>
<tr>
<td>Communication failure occurs between Cisco Unified Communications Manager and device.</td>
<td>When communication fails between a device and the Cisco Unified Communications Manager that controls it, the device recognizes the failure and maintains active connections. The Cisco Unified Communications Manager recognizes the communication failure and clears call-processing entities that are associated with calls in the device where communication was lost. The Cisco Unified Communications Managers still maintain control of the surviving devices that are associated with the affected calls. Cisco Unified Communications Manager maintains affected active calls until the end user hangs up or until the devices can determine that the media connection has been released. Users cannot invoke any call-processing features for calls that are maintained as a result of this failure.</td>
</tr>
<tr>
<td>Device failure (Phone, gateway, conference bridge, transcoder, MTP)</td>
<td>When a device fails, the connections that exist through the device stop streaming media. The active Cisco Unified Communications Manager recognizes the device failure and clears call-processing entities that are associated with calls in the failed device. The Cisco Unified Communications Managers maintain control of the surviving devices that are associated with the affected calls. Cisco Unified Communications Manager maintains the active connections (calls) that are associated with the surviving devices until the surviving end users hang up or until the surviving devices can determine that the media connection has been released.</td>
</tr>
</tbody>
</table>
CHAPTER 12

Autoregistration

This chapter provides information about Autoregistration which automatically assigns directory numbers to new devices as they connect to the Cisco Unified Communications network.

- Configure Autoregistration, page 125
- Autoregistration overview, page 126
- Autoregistration with multiple protocol support, page 127

Configure Autoregistration

Use autoregistration if you want Cisco Unified Communications Manager automatically to assign directory numbers to new phones when you plug these phones in to your network. Cisco recommends you use autoregistration to add fewer than 100 phones to your network.

Cisco Unified Communications Manager disables autoregistration by default to prevent unauthorized connections to your network. Do not enable autoregistration unless you know what your dial plan looks like, including calling search spaces and partitions.

Caution

Enabling autoregistration carries a security risk in that “rogue” phones can automatically register with Cisco Unified Communications Manager. You should enable autoregistration only for brief periods when you want to perform bulk phone adds.

Caution

Configuring mixed-mode, clusterwide security through the Cisco CTL client automatically disables autoregistration. If you want to use autoregistration and you have configured security, you must change the clusterwide security mode to nonsecure through the Cisco CTL client.

The general steps and guidelines for using autoregistration are as follows. For more information on autoregistration, see the Autoregistration overview, on page 126.
**Procedure**

**Step 1**  
In the Enterprise Parameters Configuration window, set the Auto Registration Phone Protocol to SIP or SCCP. SCCP acts as the default, so change this setting when you are auto registering phones that are running SIP.

**Step 2**  
Configure a calling search space specifically for autoregistration. For example, you can use the autoregistration calling search space to limit auto-registered phones to internal calls only.  
*Partitions and calling search spaces, on page 135*

**Step 3**  
Configure the default device pool for autoregistration by assigning the Default Cisco Unified Communications Manager Group and autoregistration calling search space to it. If you are configuring a separate default device pool for each device type, assign the default device pools to the device by using the Device Defaults Configuration window.  
*System-level configuration settings, on page 29*

**Step 4**  
Enable autoregistration only during brief periods when you want to install and autoregister new devices (preferably when overall system usage is at a minimum). During other periods, turn autoregistration off to prevent unauthorized devices from registering with Cisco Unified Communications Manager.

**Step 5**  
Install the devices that you want to autoregister.  
See the installation instructions that come with your IP phones and gateways.

**Step 6**  
Reconfigure the autoregistered devices and assign them to their permanent device pools.

**Step 7**  
In the Enterprise Parameters Configuration window, set the Auto Registration Phone Protocol setting to SIP or SCCP, whichever is needed. If auto registering more phones with a different protocol is required, repeat the preceding steps.

---

**Autoregistration overview**

Use autoregistration if you want Cisco Unified Communications Manager automatically to assign directory numbers to new phones when you plug these phones in to your network. Cisco recommends you use autoregistration to add fewer than 100 phones to your network.

Cisco Unified Communications Manager disables autoregistration by default to prevent unauthorized connections to your network. Do not enable autoregistration unless you know what your dial plan looks like, including calling search spaces and partitions.

⚠️ **Caution**

Enabling autoregistration carries a security risk in that “rogue” phones can automatically register with Cisco Unified Communications Manager. You should enable autoregistration only for brief periods when you want to perform bulk phone adds.

Configuring mixed-mode, clusterwide security through the Cisco CTL client automatically disables autoregistration. If you want to use autoregistration and you have configured security, you must change the clusterwide security mode to nonsecure through the Cisco CTL client.

Another strategy for preventing unauthorized phones from connecting to your network entails creating a Rogue device pool that allows only 911 (emergency) and 0 (operator) calls. This device pool allows phones to register but limits them to emergency and operator calls. This device pool prevents unauthorized access to phones that continuously boot in an attempt to register in your network.
When you enable autoregistration, you specify a range of directory numbers that Cisco Unified Communications Manager can assign to new phones as they connect to your network. As new phones connect to the network, Cisco Unified Communications Manager assigns the next available directory number in the specified range. After a directory number is assigned to an autoregistered phone, you can move the phone to a new location, and its directory number remains the same. If all the autoregistration directory numbers are consumed, no additional phones can autoregister with Cisco Unified Communications Manager.

The Cisco Unified Communications Manager Group that has the Auto-registration Cisco Unified Communications Manager Group check box checked, specifies the list of Cisco Unified Communications Managers that the phone will use to attempt to auto register. Ensure at least one Cisco Unified Communications Manager is selected in the group. The first Cisco Unified Communications Manager in the selected list also must have the Auto-registration Disabled on this Cisco Unified Communications Manager check box unchecked in the Cisco Unified Communications Manager Configuration window. This ensures that the Cisco Unified Communications Manager allows the autoregistration request from the phone.

New phones autoregister with the primary Cisco Unified Communications Manager in the Cisco Unified Communications Manager group that has enabled the Auto-Registration Cisco Unified Communications Manager Group setting. That Cisco Unified Communications Manager automatically assigns each auto-registered phone to a default device pool based on the device type. After a phone auto-registers, you can update its configuration and assign it to a different device pool and a different Cisco Unified Communications Manager.

Related Topics

- System-level configuration settings, on page 29
- Device pools, on page 45

**Autoregistration with multiple protocol support**

Autoregistration means that unknown phones will be coming into the network. Because the phones are unknown, Cisco Unified Communications Manager does not know whether the new phones should be registered as phones that are running SIP or as phones that are running SCCP; therefore, the system administrator uses Cisco Unified Communications Manager Administration to specify the default protocol that new phones should use for autoregistration.

Cisco devices that support both SIP and SCCP (Cisco Unified IP Phone 7905, 7911, 7912, 7940, 7941, 7960, 7961, 7970, and 7971) will auto register with the protocol that is specified in the Auto Registration Phone Protocol Enterprise Parameter. Cisco devices that only support a single protocol will auto register with that protocol regardless of the Auto Registration Phone Protocol setting. For example, the Cisco Unified IP Phone 7902 only supports SCCP. If a Cisco Unified IP Phone 7902 auto registers, it will use the SCCP regardless of whether the Auto Registration Phone Protocol is set to SIP.

**Note**

To ensure that autoregistration works correctly, ensure the Device Defaults Configuration window specifies the correct phone image names for SIP and SCCP.

To deploy phones in a mixed-protocol environment, you must perform additional steps when autoregistering a new mixed batch of phones. The first step requires that the administrator set the Cisco Unified Communications Manager Auto Registration Phone Protocol parameter in the Enterprise Parameters Configuration window to SCCP and install all the phones that are running SCCP. The second step requires that the administrator change the Auto Registration Phone Protocol parameter to SIP and autoregister all the phones that are running SIP.
Autoregistration with multiple protocol support
Dynamic Host Configuration Protocol

This chapter provides information about Dynamic Host Configuration Protocol (DHCP) server which enables Cisco Unified IP Phones, connected to either the customer data or voice Ethernet network, to dynamically obtain their IP addresses and configuration information. It uses Domain Name System (DNS) to resolve host names both within and outside the cluster.

- DHCP server, page 129
- Domain Name System, page 130
- Configure DHCP server, page 131
- TFTP server device identification, page 131
- Migration, page 131
- Alarms, page 131

DHCP server

Because DHCP server is a standalone server, no backup server exists in case the Cisco Unified Communications Manager that is configured as DHCP server fails.

Cisco Unified Communications Manager administrator configures the DHCP servers and subnets. You can configure one server for each node and multiple subnets for each server.

You must update the DNS server with the appropriate Cisco Unified Communications Manager name and address information before using that information to configure the Cisco Unified Communications Manager server.

For Cisco Unified Communications Manager, you must reboot the node if an IP address changes. As long as the node is up, it will keep refreshing the lease period for which the DHCP server provides an IP address, and hence retain the same IP address. However, hostname of the node must remain the same, even if the IP address changes.
Domain Name System

Two types of implementations exist for DNS.

- Corporate DNS, if available
- Internal DDNS service transparent to the user

The Cisco Unified Communications Manager Administration provides support to configure different scopes for the DHCP server. For each scope, you can enter a range of IP addresses and subnet masks and you can also configure options.

For configuring DNS with Corporate DNS, the corporate DNS infrastructure is used, and default DNS configuration will act as a cache only service to this corporate DNS service.

When no corporate DNS service exists, Dynamic Domain Name System (DDNS) service, a service that allows dynamic updates to hostname and IP addresses, is used to implement a clusterwide DNS infrastructure. This also serves other devices on the network that are interacting with the cluster. Each node has DNS running on it. These DNS servers get configured with hostname and IP address information for all the nodes and any other devices in the cluster. The DNS on the first node in the cluster gets configured as primary DNS, while all other nodes get configured as secondary nodes.

When any change to DNS configuration occurs to the first node of Cisco Unified Communications Manager, the change automatically gets transferred to other nodes. Other devices in the network can point to any of the nodes in the cluster for the DNS lookups.

Note

Any change to the host name of a node will require the node to be reinserted in the cluster. Before you change the host name of a node, review the document, Changing the IP Address and Host Name for Cisco Unified Communications Manager Release 8.5(1).

When nodes are being configured using by DHCP, the DHCP client on the node will get configured to dynamically update DDNS.

Whenever nodes are configured by using DHCP, one the following events occurs:

- The corporate DNS can accept dynamic updates.
- DNS gets updated within the cluster
- DHCP configuration for the nodes gets tied with their MAC addresses of the node for which you are requesting an IP address. If the node requests an IP address again, DHCP matches the MAC address to the previous request and provides the same IP address.

You must update the DNS server with the appropriate Cisco Unified Communications Manager name and address information before using that information to configure the Cisco Unified Communications Manager server.

Caution

If the AAAA record or A record do not map correctly, calls may fail.
Configure DHCP server

Use the following steps to configure DHCP Process:

**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Enable the DHCP functionality from the serviceability window.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Verify the DHCP monitor process is started on the node where the DHCP is enabled.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Use Cisco Unified Communications Manager Administration to configure the scopes and options.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Verify that configuration is captured in the /etc/dhcpd.conf file of targeted Cisco Unified Communications Manager.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Verify the DHCP server daemon is running with new configuration.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Make sure DHCP monitor process logs at the specific trace settings.</td>
</tr>
<tr>
<td>Step 7</td>
<td>Make sure the error alarm is raised when the DHCP daemon is stopped and the info alarm is raised when the daemon is restarted.</td>
</tr>
</tbody>
</table>

**TFTP server device identification**

For information about the TFTP server, see Configure TFTP, on page 106.

**Migration**

Because no migration is provided from Window 2000 based DHCP configuration to the DHCP configuration, the administrator must reconfigure the system.

**Alarms**

Two alarms get generated for DHCP.

- CiscoDhcpdFailure
- CiscoDhcpdRestarted
PART III

Dial plan architecture

• Partitions and calling search spaces, page 135
• Time-of-day routing, page 139
• Understanding route plans, page 143
• Directory numbers, page 191
• Dial rules overview, page 203
• URI dialing, page 211
Partitions and calling search spaces

This chapter provides information about partitions and calling search spaces which provide the capability for implementing calling restrictions and creating closed dial plan groups on the same Cisco Unified Communications Manager.

- Partition and call search spaces, page 135
- Guidelines and tips, page 137
- Dependency records, page 137
- Partition name limitations, page 137

Partition and call search spaces

A partition comprises a logical grouping of directory numbers (DNs) and route patterns with similar reachability characteristics. Devices that are typically placed in partitions include DNs and route patterns. These entities associate with DNs that users dial. For simplicity, partition names usually reflect their characteristics, such as “NYLongDistancePT”, “NY911PT,” and so on.

A calling search space comprises an ordered list of partitions that users can look at before users are allowed to place a call. Calling search spaces determine the partitions that calling devices, including IP phones, softphones, and gateways, can search when attempting to complete a call.

When a calling search space is assigned to a device, the list of partitions in the calling search space comprises only the partitions that the device is allowed to reach. All other DNs that are in partitions that are not in the device calling search space receive a busy signal.

Partitions and calling search spaces address three specific problems:

- Routing by geographical location
- Routing by tenant
- Routing by class of user

Partitions and calling search spaces provide a way to segregate the global dialable address space. The global dialable address space comprises the complete set of dialing patterns to which Cisco Unified Communications Manager can respond.
Partitions do not significantly impact the performance of digit analysis, but every partition that is specified in a calling device search space does require that an additional analysis pass through the analysis data structures. The digit analysis process looks through every partition in a calling search space for the best match. The order of the partitions that are listed in the calling search space serves only to break ties when equally good matches occur in two different partitions. If no partition is specified for a pattern, the pattern goes in the null partition to resolve dialed digits. Digit analysis always looks through the null partition last.

You can associate partitions with a time schedule and a time zone. Associating a partition to a time schedule and a time zone allows configuration of time-of-day routing for calls that are coming into a partition and the associated calling search spaces of the partition. See “Time-of-Day Routing” for more information.

If you configure a calling search space both on an IP phone line and on the device (IP phone) itself, Cisco Unified Communications Manager concatenates the two calling search spaces and places the line calling search space in front of the device calling search space. If the same route pattern appears in two partitions, one contained in the line calling search space and one contained in the device calling search space, Cisco Unified Communications Manager selects the route pattern that is listed first in the concatenated list of partitions (in this case, the route pattern that is associated with the line calling search space).

Note
Cisco recommends avoiding the configuration of equally matching patterns in partitions that are part of the same calling search space or part of different calling search spaces that are configured on the same phone. This practice avoids the difficulties that are related to predicting dial plan routing when the calling search space partition order is used as a tie breaker.

Before you configure any partitions or calling search spaces, all directory numbers (DN) reside in a special partition named <None>, and all devices are assigned a calling search space also named <None>. When you create custom partitions and calling search spaces, any calling search space that you create also contains the <None> partition, while the <None> calling search space contains only the <None> partition.

Note
Any device that is making a call can explicitly reach any dial plan entry that is left in the <None> partition. To avoid unexpected results, Cisco recommends that you do not leave dial plan entries in the <None> partition.

Examples
Calling search spaces determine partitions that calling devices search when they are attempting to complete a call.

For example, assume a calling search space that is named “Executive” includes four partitions: NYLongDistance, NYInternational, NYLocalCall, and NY911. Assume that another calling search space that is named “Guest” includes two partitions, NY911 and NYLocalCall.

If the Cisco Unified IP Phone that is associated with a phone or line is in the “Executive” calling search space, the search looks at partitions “NYLongDistance,” “NYInternational,” “NYLocalCall,” and “NY911” when it attempts to initiate the call. Users who are calling from this number can place international calls, long-distance calls, local calls, and calls to 911.

If the Cisco Unified IP Phone that is associated with a phone or line is in the “Guest” calling search space, the search looks only at the “NYLocalCall” and “NY911” partitions when it initiates the call. If a user who is calling from this number tries to dial an international number, a match does not occur, and the system cannot route the call.
Guidelines and tips

Use the following tips and guidelines when you are setting up partitions and calling search spaces:

- Use concise and descriptive names for your partitions. The *CompanynameLocationCalltypePT* format usually provides a sufficient level of detail and is short enough to enable you to quickly and easily identify a partition. For example, “CiscoDallasMetroPT” identifies a partition for toll-free inter-LATA (local access and transport area) calls from the Cisco office in Dallas.

- To ensure that dialing privileges are uniform for all lines on a given phone, you may configure the calling search space on the IP phone itself and not on the individual lines of the phone. This practice prevents users from choosing another line on the phone to bypass calling restrictions.

- When you are configuring call forward features on an IP phone line, do not choose a calling search space that can reach the PSTN. This practice prevents users from forwarding their IP phone lines to a long-distance number and dialing their local IP phone number to bypass long-distance toll charges.

Related Topics

- Partition name limitations, on page 137
- Local route groups and called party transformations, on page 151

Dependency records

If you need to find specific information about partitions and calling search spaces, click the Dependency Records link that is provided in the Related Links drop-down list box that is on the Cisco Unified Communications Manager Administration Partition Configuration and Calling Search Space Configuration windows. If the dependency records are not enabled for the system, the dependency records summary window displays a message.

Partition Dependency Records

The Dependency Records Summary window for partitions displays information about calling search spaces, route patterns, and directory numbers that are using the partition. To find more information, click the record type, and the Dependency Records Details window displays.

Calling Search Space

The Dependency Records Summary window for calling search spaces displays information about phones, gateways, voice-mail ports, and device pools that are using the calling search space. To find more information, click the record type, and the Dependency Records Details window displays.

Related Topics

- Local route groups and called party transformations, on page 151

Partition name limitations

A calling search space (CSS) clause that call processing uses internally limits the maximum number of partitions. The CSS clause comprises the list of partitions in the calling search space by name. The CSS clause
that call processing uses comprises a combination of a device CSS and the CSS for the directory number (DN) or route pattern that is associated with the device (for example, a line on a phone).

The maximum length of the combined CSS clause (device and pattern) comprises 1024 characters, including separator characters between partition names (for example, “partition 1:partition 2:partition 3”). Because the CSS clause uses partition names, the maximum number of partitions in a CSS varies depending on the length of the partition names. Also, because the CSS clause combines the CSS of the device and the CSS of the route pattern, the maximum character limit for an individual CSS specifies 512 (half of the combined CSS clause limit of 1024 characters).

When you are creating partitions and calling search spaces, keep the names of partitions short relative to the number of partitions that you plan to include in a calling search space.

Related Topics

- Guidelines and tips, on page 137
- Local route groups and called party transformations, on page 151
Time-of-day routing

This chapter provides information about Time-of-Day routing which routes calls to different locations based on the time of day when a call is made. For example, during business hours, calls can route to an office, and after hours, calls can go directly to a voice-messaging system or to a home number.

- Time-of-day routing, page 139
- End-users and time-of-day routing, page 141
- Dependency records, page 141

Time-of-day routing

Time-of-Day routing comprises individual time periods that the administrator defines and groups into time schedules. The administrator associates time schedules with a partition. In the Partition Configuration window, the administrator chooses either the time zone of the originating device or any specific time zone for a time schedule. The system checks the chosen time zone against the time schedule when the call gets placed to directory numbers in this partition. The Time Period and Time Schedule menu items exist in the Call Routing menu under the Class of Control submenu. The Partition and Calling Search Space menu items also have moved to the Class of Control submenu.

Time periods

A time period comprises a start time and end time. The available start times and end times comprise 15-minute intervals on a 24-hour clock from 00:00 to 24:00. Additionally, a time period requires definition of a repetition interval. Repetition intervals comprise the days of the week (for example, Monday through Friday) or a day of the calendar year (for example, June 9).

Examples

You can define time period \textit{weekdayofficehours} as 08:00 to 17:00 from Monday to Friday.

You can define time period \textit{newyearsday} as 00:00 to 24:00 on January 1.

You can define time period \textit{noofficehours} that has no office hours on Wednesdays. For this time period, the associated partition is not active on Wednesdays.
In defining a time period, the start time must precede (be less than) the end time.

Tip
To define an overnight time span that starts on Monday through Friday at 22:00 and ends at 04:00 the next morning, create two time periods, such as lateevening (from 22:00 to 24:00 on Monday through Friday) and earlymorning (from 00:00 to 04:00 on Tuesday through Saturday). Use the Time Schedule Configuration window to associate the lateevening and earlymorning time periods into a single time schedule that spans the overnight hours.

After the administrator creates a time period, the administrator must associate the time period with a time schedule.

Time period behavior
If you define a time period with a specific date, on that specified date, that period overrides other periods that are defined on a weekly basis.

Example
Consider the following example:

- A time period, afterofficehours, that is defined as 00:00 to 08:00 from Monday to Friday exists.
- A time period, newyearseve, that is defined as 14:00 to 17:00 on December 31st exists.

In this case, on December 31st, the afterofficehours period will not be considered because it gets overridden by the more specific newyearseve period.

Time schedules
A time schedule comprises a group of defined time periods that the administrator associates. After the administrator has configured a time period, the time period displays in the Available Time Periods list box in the Time Schedule Configuration window. The administrator can select a time period and add it to the Selected Time Periods list box.

Note
After the administrator selects a time period for association with a time schedule, the time period remains available for association with other time schedules.

After the administrator has configured a time schedule, the administrator can use the Partition Configuration window to select either the time zone of the originating device or any specific time zone for a defined time schedule. The selected time zone gets checked against the time schedule when the user places the call.

The Time-of-Day feature filters the CallingSearchSpace string through Time-of-day settings that are defined for each partition in the CallingSearchSpace.

After time-of-day routing is configured, if the time of an incoming call is within one of the time periods in the time schedule, the partition gets included in the filtered partition list search for the call.
Examples
You can define time schedule USAholidays as the group of the following time periods: newyearsday, presidentsday, memorialday, independenceday, laborday, thanksgivingday, christmasday. The administrator must first configure the applicable time periods.

You can define time schedule library_open_hours as the group of the following time periods: Mon_to_Fri_hours, Sat_hours, Sun_hours. The administrator must first configure the applicable time periods.

End-users and time-of-day routing
If time-of-day routing is enforced, users cannot set certain CFwdAll numbers at certain times. For example, User A Calling Search Space for forwarding includes a Time-of-Day-configured partition that allows international calls from 08:00 to 17:00 (5:00 pm). User A wants to configure his CFwdAll number to an international number. He can only set this number during the 08:00-to-17:00 time period because, outside these hours, the system does not find the international number in the partition that is used to validate the CFwdAll number.

If the user sets the CFwdAll during office hours when it is allowed, and the user receives a call outside office hours, the caller hears fast-busy.

Users cannot reach directory numbers in some partitions that are configured for time-of-day routing and that are not active during the time of call, depending upon the configuration of partitions.

Users also cannot reach the Route/Translation pattern in partitions configured with time-of-day routing which is not active at the time of call.

Although a user may not be able to set Forward All for a phone due to the partition and time-of-day settings that apply to the phone, an administrator or a user can still set the Call Forward All option on the phone from the Cisco Unified Communications Manager Administration page.

TOD settings comes into effect when the lines are included in a Hunt List. The settings only apply to the Hunt Pilot and not to the lines within that Hunt List.

Dependency records
If you need to find specific information about time periods and time schedules, choose Dependency Records from the Related Links drop-down list box that is provided on the Cisco Unified Communications Manager Administration Time Period Configuration and Time Schedule Configuration windows. If the dependency records are not enabled for the system, the dependency records summary window displays a message.

The Dependency Records Summary window for time periods displays information about time schedules that are using the time period. To find more information, click the record type, and the Dependency Records Details window displays.
Time Schedule Dependency Records

The Dependency Records Summary window for time schedules displays information about partitions that are using the time schedule. To find more information, click the record type, and the Dependency Records Details window displays.
Understanding route plans

This chapter provides information about the Route Plan drop-down list on the menu bar which allows you to configure Cisco Unified Communications Manager route plans by using route patterns, route filters, route lists, and route groups, as well as hunt pilots, hunt lists, and line groups.

- Automated Alternate Routing, page 144
- Route plan overview, page 146
- Route groups and route lists, page 147
- Route patterns, page 148
- Local route groups and called party transformations, page 151
- Line groups, page 152
- Hunt lists, page 152
- Hunt pilots, page 152
- Call coverage, page 153
- Log out of hunt groups, page 154
- Closest match routing, page 156
- Use wildcard character in route patterns, page 157
- Translation patterns, page 157
- Static digit analysis, page 158
- Calling party normalization, page 160
- Special characters and settings, page 161
- Calling and Called party transformations, page 177
- Caller Identification and restriction, page 184
- Route plan report, page 189
Automated Alternate Routing

Automated alternate routing (AAR) provides a mechanism to reroute calls through the PSTN or other network by using an alternate number. As a subset of the AAR feature, Cisco Unified Communications Manager automatically reroutes calls through the PSTN or other networks when Cisco Unified Communications Manager blocks a call due to insufficient location bandwidth. With automated alternate routing, the caller does not need to hang up and redial the called party.

When a call is made from the device of one location to the device of another location, location bandwidth gets deducted from the maximum available bandwidth that is available for the call at either location. If not enough location bandwidth for the call exists at either location, instead of blocking the call, Cisco Unified Communications Manager uses the table of AAR groups and the external number of the terminating directory number to supply the alternate number that is used to reroute the call through the PSTN or other network. The Cisco Unified IP Phone displays the message “Network congestion, rerouting.” (Configure this message by using Service Parameters Configuration for the Cisco CallManager service.) Cisco Unified Communications Manager automatically attempts to reroute the call by using the alternate number. If the reroute is successful, the caller connects to the called party.

AAR supports the following call scenarios for insufficient bandwidth:

- Call originates from a line or directory number (DN) of an IP phone within one location and terminates to a line or DN of another IP phone within another location. This scenario includes calls that terminate at the shared line with terminating IP phone devices that are resident in multiple locations and calls that terminate at the Cisco voice-mail port.

- Incoming call through a gateway device within one location terminates to a line or DN of an IP phone within another location. This scenario includes calls that terminate at the shared line with terminating IP phone devices that are resident in multiple locations and calls that terminate at the Cisco voice-mail port.

Cisco Unified Communications Manager automatically attempts to reroute calls, due to insufficient bandwidth, through the PSTN or other network only when the Automated Alternate Routing Enable enterprise parameter is set to true. Cisco Unified Communications Manager uses the device-based AAR calling search space, which is assigned to Cisco Unified IP Phone station devices and gateway devices, when it attempts to route the call to the gateway device that connects to the PSTN or other network. Cisco Unified Communications Manager uses the external phone number mask and the directory number of the line or DN and the Cisco voice-mail port to derive the alternate number that is used to reroute the call.

Automated Alternate Routing Example

In the following scenario, line/DN 5000 in the Richardson AAR group calls line 5001 in the San Jose AAR group. If not enough location bandwidth exists, the call attempts to reroute through the PSTN or other network. To route the call from AAR group Richardson to AAR group San Jose, Cisco Unified Communications Manager needs to know the access digit(s) to dial out to the PSTN or other network, the long-distance dialing requirement, if any, and the alternate number. Cisco Unified Communications Manager retrieves the information from the AAR dial prefix matrix table, which is indexed by the originating line AAR group value and the terminating line AAR group value. The following shows how the AAR group field is data filled in the line/DN table:
Table 11: Line/DN and AAR Group Association

<table>
<thead>
<tr>
<th>Line/DN</th>
<th>AAR Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>5000</td>
<td>Richardson</td>
</tr>
<tr>
<td>5001</td>
<td>San Jose</td>
</tr>
<tr>
<td>5002</td>
<td>Dallas</td>
</tr>
</tbody>
</table>

Cisco Unified Communications Manager retrieves the prefix digits from the AAR dial prefix matrix table based on the AAR group value of the originating line/DN and gateway device and the AAR group value of the terminating line, and Cisco voice-mail port, to transform the derived alternate number. The following shows an example of how the AAR dial prefix matrix table is data filled:

Table 12: AAR Dial Prefix Matrix Table Example

<table>
<thead>
<tr>
<th>From AAR Group</th>
<th>To AAR Group</th>
<th>Prefix Digits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Richardson</td>
<td>San Jose</td>
<td>91</td>
</tr>
<tr>
<td>Richardson</td>
<td>Dallas</td>
<td>9</td>
</tr>
<tr>
<td>Richardson</td>
<td>Richardson</td>
<td>9</td>
</tr>
<tr>
<td>San Jose</td>
<td>Richardson</td>
<td>91</td>
</tr>
<tr>
<td>San Jose</td>
<td>Dallas</td>
<td>91</td>
</tr>
<tr>
<td>San Jose</td>
<td>San Jose</td>
<td>9</td>
</tr>
<tr>
<td>Dallas</td>
<td>Richardson</td>
<td>9</td>
</tr>
<tr>
<td>Dallas</td>
<td>San Jose</td>
<td>91</td>
</tr>
<tr>
<td>Dallas</td>
<td>Dallas</td>
<td>9</td>
</tr>
</tbody>
</table>

Cisco Unified Communications Manager prepends the prefix digits that are retrieved from the AAR dial prefix matrix table to the derived alternate number. Digit analysis uses the transformed digits, plus the AAR calling search space, to route the call to the PSTN or other network.

A much greater rate of success for automated alternate routing occurs when a gateway is located in the same location as the originating or terminating device. Therefore, a call that is outgoing to the PSTN or other network from a gateway that is located in the same location as the originating device and that is also incoming from a gateway located in the same location as the terminating device describes the best scenario. In other scenarios, the call remains subject to location bandwidth validation between the originating device and outgoing gateway, and between the terminating device and incoming gateway.
Automated Alternate Routing enable service parameter

Besides configuring AAR groups, ensure that the Automated Alternate Routing Enable clusterwide service parameter is set to True. (The default value for this service parameter specifies False.)

The Clusterwide Parameters (System - CCMAutomated Alternate Routing) section of the service parameters for the Cisco CallManager service includes the parameter.

Automated Alternate Routing and hunt pilots

In previous Cisco Unified Communications Manager releases, if the voice-messaging system is in a central location and the user is in a remote location, when the remote user tries to reach the voice-messaging system and bandwidth is not available on the WAN link, Cisco Unified Communications Manager can reroute the call through the PSTN to the voice-messaging system.

In the current Cisco Unified Communications Manager release, AAR does not automatically work with hunt pilots. Because the fully qualified directory number (DN) of the remote agent is unknown, AAR cannot initiate the reroute.

To enable AAR to work with hunt pilots, two additional fields display in the Hunt Pilot Configuration window: AAR Group and External Number Mask. For each hunt pilot, you must configure these fields in the Hunt Pilot Configuration window for AAR groups to work with hunt pilots.

Automated Alternate Routing and remote gateways

AAR exhibits the limitation that calls routed over a remote gateway during a high-bandwidth situation fail, and the calls cannot be routed over the local gateway when AAR is used. This functionality is important to customers who use Tail-End Hop Off (TEHO) for toll bypass.

See the Troubleshooting Guide for Cisco Unified Communications Manager for details of a workaround to avoid the use of AAR in remote-gateway, high-bandwidth situations.

Route plan overview

Cisco Unified Communications Manager uses route plans to route internal calls, and to route external calls to a private network or the public switched telephone network (PSTN).

Route patterns, route filters, route lists, route groups, line groups, hunt lists, and hunt pilots provide flexibility in network design. Route patterns work in conjunction with route filters to direct calls to specific devices and to include or exclude specific digit patterns. Use route patterns to include and exclude digit patterns. Use route filters primarily to include digit patterns. Route lists control the selection order of the route groups. Route groups set the selection order of the gateway devices.

You can assign route patterns to gateways, to trunks, or to a route list that contains one or more route groups. Route groups determine the order of preference for gateway and trunk usage. Route groups allow overflows from busy or failed devices to alternate devices.

Route lists determine the order of preference for route group usage. If a route list is configured, you must configure at least one route group. One or more route lists can point to one or more route groups.

Route filters may restrict certain numbers that are otherwise allowed by a route pattern from being routed. Tags, or clauses, provide the core component of route filters. A tag applies a name to a portion of the dialed
digits. For example, the North American Numbering Plan (NANP) number 972-555-1234 contains the LOCAL-AREA-CODE (972), OFFICE-CODE (555), and SUBSCRIBER (1234) tags.

**Note**
The NANP designates the numbering plan for the PSTN in the United States and its territories, Canada, Bermuda, and many Caribbean nations. NANP includes any number that can be dialed and is recognized in North America.

Route patterns represent all valid digit strings. Cisco Analog Access Trunk Gateways, Cisco Digital Access Trunk Gateways, Cisco MGCP gateways, H.323-compliant gateways, and trunks also use route patterns. Cisco gateways can route ranges of numbers with complex restrictions and manipulate directory numbers before the Cisco Unified Communications Manager passes them on to an adjacent system. The adjacent system can include a central office (CO), a private branch exchange (PBX), or a gateway on another Cisco Unified Communications Manager system.

A line group comprises a list of DNs. Line groups specify a distribution algorithm (such as Top Down) for the members of the line group. Line groups also specify the hunt options to use in cases where the line group members do not answer, are busy, or are not available. A directory number may belong to more than one line group.

Hunt lists comprise ordered groupings of line groups. A line group may belong to more than one hunt list. A hunt list must specify at least one line group before the hunt list can accept calls.

Hunt pilots represent route patterns that are used for hunting. A hunt pilot can specify a partition, numbering plan, route filter, and hunt forward settings. A hunt pilot must specify a hunt list.

**Related Topics**

- Gateways dial plans and route groups, on page 374

**Route groups and route lists**

Route groups contain one or more devices, and route lists contain one or more route groups. Cisco Unified Communications Manager may restrict the gateways that you can include in the same route group and the route groups that you can include in the same route list. For the purpose of route group and route list restrictions, Cisco Unified Communications Manager divides gateways into three types:

- Type 1-MGCP QSIG gateways and QSIG-enabled intercluster trunks
- Type 2-MGCP non-QSIG, Skinny, T1-CAS gateways; non-QSIG intercluster trunks
- Type 3-H.225 and H.323 gateways, and all other trunk types

Route lists can contain a mixture of route group types, although you cannot combine an H225 trunk with a Type 1 (QSIG) route group. Cisco Unified Communications Manager does not allow you to add route groups that contain gateways that use the H.323 or H.225 protocol (Type 3) and route groups that contain MGCP gateways that use a QSIG protocol (Type 1) to the same route list. You can create route lists with any
combination of Type 1 route groups and Type 2 route groups as well as with any combination of Type 2 route groups and Type 3 route groups, as illustrated below.

**Figure 17: Valid Route Lists Example**

You cannot combine route groups and line groups, and route lists and hunt lists become separate entities. Thus, route groups make up route lists, and line groups make up hunt lists. If an existing route/hunt list includes a line group as a member, Cisco Unified Communications Manager migrates the route/hunt list to a hunt list.

Route lists can simultaneously run on all nodes and Cisco Unified Communications Manager can randomly choose from any of the available route lists that can reach a given node. The system ensures that, over time and on average, all 16 nodes in the core cluster are used equally. This prevents system resources on some nodes from being idle while other nodes are dealing with an unsustainable call burden.

**Route patterns**

Cisco Unified Communications Manager uses route patterns to route or block both internal and external calls.

Route group and route lists are part of route pattern configuration. Line groups and hunt lists are part of hunt pilot configuration. Route patterns and hunt pilots are configured separately. Route groups or route lists cannot be added to hunt pilot and line groups. Hunt lists cannot be added to route pattern. If an existing route pattern/hunt pilot associates with a hunt list, Cisco Unified Communications Manager migrates the route pattern/hunt pilot to a hunt pilot.

The simplest route pattern specifies a set of one or more digits. For example, the number 8912 specifies a route pattern.

Gateways and Cisco Unified IP Phones can also use more complex route patterns that can contain wildcards. A wildcard represents a range of numbers; for example, X represents any digit 0 through 9.

To classify a call as OnNet or OffNet, administrators can set the Call Classification field to OnNet or OffNet, respectively, on the Route Pattern Configuration window. Administrators can override the route pattern setting and use the trunk or gateway setting by checking the Allow Device Override check box on the Route Pattern Configuration window.
If a gateway has no route pattern that is associated with it, or it does not belong to a route group, it cannot route any calls.

You can use route patterns to invoke network-specific services/facilities on a call-by-call basis by configuring the fields in the ISDN Network-Specific Facilities Information Element section on the Route Pattern Configuration window. Cisco Unified Communications Manager uses the network-specific services/facilities when the user dials the route pattern.

Note

Cisco Unified Communications Manager only uses the network-specific information with PRI protocol gateways. H.323 gateways do not support network-specific facilities, but they support SDN when the dial peers are configured accordingly. Cisco Unified Communications Manager codes the bearer capability as Speech for the ACCUNET service.

RoutePattern usage

You can assign a route pattern directly to a Cisco Access Gateway, or you can assign it to a route list for more flexibility. For example, the figure shows Cisco Digital Access Gateway 1 designated as the first choice for routing outgoing calls to the PSTN when a matching route pattern is dialed.

Tip

If a gateway does not have a route pattern, it cannot place calls to the PSTN or to a PBX. To assign a route pattern to an individual port on a gateway, you must assign a route list and a route group to that port.
The following figure shows the effects of using route patterns with Cisco Digital Gateways. This example assigns the route pattern to a route list, and that route list associates with a single route group. The route group supports a list of devices that are selected based on availability.

**Figure 18: Route Plan Summary Diagram for Cisco Digital Gateways**

When the system initially presents a call to a member of a route list, Cisco Unified Communications Manager reroutes for all cause codes other than Out of Bandwidth, User Busy, and Unallocated Number. The value of the associated service parameters for the Cisco CallManager service determines the rerouting decision for those cause codes. The Clusterwide Parameters (Route Plan) grouping includes the Stop Routing on Out of Bandwidth Flag, Stop Routing on User Busy Flag, and Stop Routing on Unallocated Number Flag service parameters. You can set each service parameter to True or False.

After a route list locks onto a trunk, no rerouting occurs. The media connect time of the endpoints and the Stop Routing service parameters determine when a route list stops hunting for the next route group. When media negotiation begins, the route list or hunt list loses the ability to reroute.

The Stop Routing on Q.931 Disconnect Cause Code service parameter for the Cisco CallManager service determines routing behavior when a call that is being routed to a remote site through a route list gets released and a Q.931 cause code gets sent to Cisco Unified Communications Manager. If the cause code that is encountered in the message matches a cause code that this parameter specifies, a local Cisco Unified Communications Manager stops routing the call. (The call does not get sent to the next device in the route list).
If a route pattern is associated with a gateway, and all the resources of that gateway are used, then the call does not get routed.

The following figure shows the effects of using route patterns with Cisco Analog Gateways. This example assigns the route pattern to a route list, and that route list associates with two route groups. Route group 1 associates with ports 1 through 8 on gateway 1, which routes all calls to interexchange carrier 1 (IXC 1). Route group 1 also associates with ports 1 through 4 on gateway 2. Route group 2 associates with ports 5 through 8 on gateway 2 and all ports on gateway 3.

Figure 19: Route Plan Summary Diagram for Cisco Analog Access Gateways

Each route group supports a list of devices that are chosen on the basis of availability. For route group 1, if ports 1 through 8 on the first-choice gateway are busy or out of service, calls route to ports 1 through 4 on the second-choice gateway. If all routes in route group 1 are unavailable, calls route to route group 2. For route group 2, if ports 5 through 8 on the first-choice gateway are busy or out of service, calls route to ports 1 through 8 on the second-choice gateway. If no ports on any gateway in either route group are available, the call routes to an all trunks busy tone.

Local route groups and called party transformations

The Local Route Group feature helps reduce the complexity and maintenance efforts of provisioning in a centralized Cisco Unified Communications Manager deployment that uses a large number of locations. The
fundamental breakthrough in the Local Route Group feature comprises decoupling the location of a PSTN gateway from the route patterns that are used to access the gateway.

The Local Route Group feature provides the ability to reduce the number of route lists and route patterns that need to be provisioned for implementations of Cisco Unified Communications Manager where each of N sites needs to have access to the local gateways of the other N-1 remote sites. One such scenario occurs with Tail End Hop Off (TEHO).

Related Topics
    Dependency records, on page 137
    Guidelines and tips, on page 137
    Partition name limitations, on page 137

Line groups

Line groups contain one or more directory numbers. A distribution algorithm, such as Top Down, Circular, Longest Idle Time, or Broadcast, associates with a line group. Line groups also have an associated Ring No Answer reversion timeout value.

The following descriptions apply to the members of a line group:

• An idle member designates one that is not serving any call.
• An available member designates one that is serving an active call but can accept a new call(s).
• A busy member cannot accept any calls.

A directory number may belong to more than one line group.

Hunt lists

Hunt lists comprise ordered groupings of line groups. A line group may belong to more than one hunt list. Hunt pilots associate with hunt lists. A hunt list may associate with more than one hunt pilot.

Note
Configuration of hunt lists and route lists occurs separately. If an existing route/hunt list has a line group as a member, Cisco Unified Communications Manager migrates the route/hunt list to a hunt list.

Note
TOD settings comes into effect when the lines are included in a hunt list. The settings only apply to the hunt pilot and not to the lines within that hunt list.

Hunt pilots

Hunt pilots comprise sets of digits. They comprise lists of route patterns that are used for hunting. A hunt pilot can specify a partition, numbering plan, route filter, and hunt forward settings. A hunt pilot must specify a hunt list.
Configuration of hunt pilots and route patterns occurs separately. If an existing route pattern/hunt pilot associates with a hunt list, Cisco Unified Communications Manager migrates the route pattern/hunt pilot to a hunt pilot.

**Note**
TOD settings comes into effect when the lines are included in a hunt list. The settings only apply to the hunt pilot and not to the lines within that hunt list.

---

**Call coverage**

The Call Coverage feature comprises the following Cisco Unified Communications Manager capabilities:

- Forwarding provides separate configuration based on whether the call originator is an internal user or an external user. See the Internal and external calls, on page 154.
- Hunting supports personal forwarding. See the Personal preferences, on page 154.
- Route patterns and hunt pilots are separated in two different features.

**Hunting and call forwarding**

The concept of hunting differs from that of call forwarding. Hunting allows Cisco Unified Communications Manager to extend a call to one or more lists of numbers, where each such list can specify a hunting order that is chosen from a fixed set of algorithms. When a call extends to a hunt party from these lists and the party fails to answer or is busy, hunting resumes with the next hunt party. (The next hunt party varies depending on the current hunt algorithm.) Hunting thus ignores the Call Forward No Answer (CFNA), Call Forward Busy (CFB), or Call Forward All (CFA) settings for the attempted party.

Call forwarding allows detailed control as to how to extend (divert and redirect represent equivalent terms for extend) a call when a called party fails to answer or is busy and hunting is not taking place. For example, if the CFNA setting for a line is set to a hunt-pilot number, a call to that line that is not answered diverts to the hunt-pilot number and thus begins hunting.

Cisco Unified Communications Manager offers the ability to redirect a call when hunting fails (that is, when hunting terminates without any hunt party answering, due either to exhausting the list of hunt numbers or to timing out). If used, this final redirection comprises a Call Forwarding action. Therefore, the Hunt Pilot Configuration window includes Call Forwarding configuration concepts that are similar to those found on the Directory Number Configuration window.

**Example of call hunting**

Although hunting differs from forwarding, hunting often originates as a call that gets forwarded to a hunt-pilot number. The call coverage feature extends hunting to allow final forwarding after hunting either exhausts or times out.

A typical call that invokes hunting can include the following phases:

1. A call extends to the original called party.
The call forwards to hunting (for example, due to the Call Forward All [CFA], CFNA, or CFB setting for the original called line).

The call hunts through provisioned hunt groups according to provisioned algorithms for each group. Hunting either succeeds (if a hunt party answers), exhausts (if all hunt parties are attempted, but none answer), or times out (if the time specified in the Maximum Hunt Timer runs out before all parties are attempted, and none of the parties that were attempted answer).

For the purpose of this example, we assume that hunting does not succeed.

If some form of final forwarding is configured, the call forwards to a next destination; otherwise, the call gets released.

**Maximum hunt timer**

The Maximum Hunt Timer field on the Hunt Pilot Configuration window allows the administrator to enter a value (in seconds) to limit the time for hunting through a hunt list. After the specified time lapses, if hunting has not succeeded, the call gets forwarded to a voice-messaging system, a specific dialed number, or some personal treatment (if configured), or the call gets released.

**finalCalledPartyNumber field service parameter**

This service parameter for the Cisco CallManager service allows you to specify either the line group directory number (DN) that picks up a call to a hunt pilot number or the hunt pilot number as the final called party number in the Call Detail Record (CDR).

**Internal and external calls**

Forwarding provides separate configuration based on whether the originator of a call is an internal user or an external user. This distinction applies to Call Forward Busy (CFB), Call Forward No Answer (CFNA), and Call Forward No Coverage (CFNC) cases.

**Personal preferences**

Hunting supports the capability to provide a final forwarding treatment to voice-messaging system, a specific dialed number, or some personal treatment (based on the original called party) when hunting either exhausts or times out. The capability to provide separate final forwarding treatment based on whether the call was internal or external also exists. Hunting supports a separate, configurable maximum hunt timer for each hunt-pilot number.

In the Hunt Pilot configuration settings, Use Personal Preferences, Destination fields are available to enable the Call Forward No Coverage (CFNC) settings for the original called number that forwarded the call to the hunt pilot.

**Log out of hunt groups**

The Log Out of Hunt Groups feature allows users of phones that are running SCCP and phones that are running SIP to log out their phones from receiving calls that get routed to directory numbers that belong to line groups to which the phone lines are associated.
Regardless of the phone status, the phone rings normally for incoming calls that are not calls to the line group(s) that are associated with the phone.

The phone provides a visual status of the login state, so the user can determine by looking at the phone whether they are logged in to their line group(s).

System administrators can configure phones to be automatically logged into hunt groups by using the Logged Into Hunt Group check box on the Phone Configuration window in Cisco Unified Communications Manager Administration. By default, this check box gets checked for all phones. Users log in and out of hunt groups by using the HLog softkey (see the Log out of hunt groups softkey, on page 155).

Log Out of Hunt Groups has the following limitations for phones that are running SIP:

- When a phone that is running SIP (7906, 7911, 7941, 7961, 7970, and 7971) is logged into hunt groups, and Call Forward All is activated, the call gets presented to the phone that is running SIP.
- When 7940 and 7960 phones that are running SIP are logged into hunt groups, and Call Forward All is activated, the phone will get skipped and the next phone in the line group will be rung.
- 7940 and 7960 phones that are running SIP and third-party phones that are running SIP can be logged into/out of hunt groups by using the Phone Configuration window, but no softkey support exists.
- 7940 and 7960 phones that are running SIP and third-party phones that are running SIP will not show “Logged out of hunt groups” on the status line.
- 7940 and 7960 phones that are running SIP and third-party phones that are running SIP will not play the hunt group logoff notification tone regardless of whether the tone is configured.

Log out of hunt groups softkey

Cisco Unified Communications Manager provides the HLog softkey that allows a phone user to log a phone out of all line groups to which the phone directory numbers belong. The user uses the HLog softkey to toggle between logon and logoff. After the feature is enabled (logoff) on a phone, calls that come into line groups that are associated with this phone skip this phone and go directly to the next line in the hunt list.

Because the Log Out of Hunt Groups feature is device-based, when the user enables the feature by pressing the HLog softkey, the phone gets logged off from all associated line groups. If a phone has directory numbers that belong to multiple line groups, pressing the HLog softkey logs the phone out of all associated line groups. The default phone state specifies logon.

The HLog softkey does not get added to any standard softkey template, but the HLog softkey displays as a selectable softkey in the Connected, Off Hook, and On Hook states in the Cisco Unified Communications Manager Administration Softkey Layout Configuration window for a new softkey template. The HLog softkey displays on the phone when the phone is in the Connected, Off Hook, and On Hook states if the administrator adds the HLog softkey to the softkey template that the phone uses. If necessary, the softkey label gets translated to a different language.

A prompt status message displays the status of the feature when the softkey is pressed to log off, if the new softkey is selected in the Softkey Template that the device is currently using. If necessary, the prompt status message gets translated to a different language.

See the Cisco Unified Communications Manager Administration Guide for the details of configuring softkey templates in Cisco Unified Communications Manager Administration.
Hunt group logoff notification service parameter

The Hunt Group Logoff Notification service parameter in the Clusterwide Parameters (Device - Phone) section of the Service Parameters Configuration window for the Cisco CallManager service provides the option to turn audible ring tones on or off when calls that come in to a line group arrive at the phone and the current status of the phone is logoff. The default value specifies None, which causes the phone not to ring.

Non-shared-line operation

If a phone is logged out of a line group and an extension on the phone is not shared, the line group does not ring that directory number in the line group. When the line group would normally offer the call to the directory number, call processing skips the directory number and acts as if the directory number does not belong to the line group.

Shared-line operation

Because the Log Out of Hunt Group feature is device-based, when a user logs a phone out, the feature affects only the logged-out phone. Calls to a line group that contains a shared-line directory number (DN) behave as follows:

- The DN does not ring if all phones that share that DN are logged out.
- The DN does ring if one or more phone that is sharing the DN is logged in.
- The audible ring on a phone that is logged out gets turned off by default. Cisco Unified Communications Manager provides a system parameter that can be set, so a different ring tone plays when a call comes in to a logged-off hunt group member.

Closest match routing

Closest match routing process routes a call by using the route pattern that most closely matches the dialed number. When the Cisco Unified Communications Manager encounters a dialed number that matches multiple route patterns, it uses closest match routing to determine which route pattern most closely matches the number and directs the call by using that route pattern.

When two configured route patterns exactly match the same number of addresses in different partitions, Cisco Unified Communications Manager chooses the route pattern on the basis of the order in which the partitions are listed in the calling search space. (Cisco Unified Communications Manager chooses the route pattern from the partition that appears first in the calling search space.)

If two configured route patterns exactly match the same number of addresses in a partition, the Cisco Unified Communications Manager arbitrarily chooses one. The following paragraphs explain why such exact matches signify an unusual occurrence.

Several route patterns can match a single number. For instance, the number 8912 matches all the following route patterns: 8912, 89XX, and 8XXX.

In this example, the route pattern 8912 matches exactly one address. The route pattern 89XX matches 8912 plus 99 other addresses, and the route pattern 8XXX matches 8912 plus 999 other addresses.

If the user dials 8913, the call routes differently. Using the preceding example, this address matches only the routing patterns 89XX and 8XXX. Because 89XX matches a narrower range of addresses than 8XXX, the
Cisco Unified Communications Manager delivers the call to the device that is assigned the routing pattern 89XX.

Related Topics

Called party number transformations settings, on page 181

Use wildcard character in route patterns

Using the @ wildcard character in a route pattern provides a single route pattern to match all National Numbering Plan numbers, and requires additional consideration.

The number 92578912 matches both of the following route patterns: 9.@ and 9.XXXXXXX. Even though both these route patterns seem to equally match the address, the 9.@ route pattern actually provides the closest match. The @ wildcard character encompasses many different route patterns, and one of those route patterns is [2-9][02-9]XXXXX. Because the number 2578912 more closely matches [2-9][02-9]XXXXX than it does XXXXXXX, the 9.@ route pattern provides the closest match for routing.

When configuring route patterns, take the following considerations into account:

- When @ is used in a routing pattern, the system recognizes octothorpe (#) automatically as an end-of-dialing character for international calls. For routing patterns that do not use @, you must include the # in the routing pattern to be able to use the # character to signal the end of dialing.

- If the route pattern contains an at symbol (@), the Discard Digits field can specify any discard digits instructions (DDIs).

The Special characters and settings, on page 161 lists DDIs and describes the effects of applying each DDI to a dialed number.

Discard Digits Instructions

A discard digits instruction (DDI) removes a portion of the dialed digit string before passing the number on to the adjacent system. Portions of the digit string must be removed, for example, when an external access code is needed to route the call to the PSTN, but the PSTN switch does not expect that access code.

Note

With non-@ patterns, you can use only Discard Digits instructions <None>, NoDigits, and PreDot.

Translation patterns

Cisco Unified Communications Manager uses translation patterns to determine how to route a call after it is placed. Configuring translation patterns allows Cisco Unified Communications Manager to manipulate calling and called digits as appropriate. During digit analysis when Cisco Unified Communications Manager identifies that a pattern match has occurred, Cisco Unified Communications Manager uses the calling search space that is configured for the translation pattern to perform the subsequent match.

Because Cisco Unified Communications Manager supports local route groups, calling party normalization, and the international escape character +, which allow you to globalize, route, and localize calling party numbers, you can configure translation patterns as urgent or non-urgent to ensure that Cisco Unified Communications Manager does not route the call before it should be routed.
Forexample,ifacallerinthe408areacodedials95551212,thisnumbergetsglobalizedto+14085551212 throughtheuseoftranslationpatterns;thatistodigitanalysisdoesapatternmatchforthatstringtodetermine wheretoroutethecall.Inthisexample,atranslationpatterntakes9.[2-9]XXXXXX,translatesthatstringto +1408XXXXXXX,andthenmaps thatvaluetocallingsearchspacethatcontainstheglobalizedpatterns.

This example works as long as you do not use variable length dialing, as is the case with international calls. If you want to route an international call, you need a translation pattern for 9011! that disregards the predot and adds the prefix +. If you configure the translation pattern as urgent priority, 9011! matches with the first digit after the 9011 and Cisco Unified Communications Manager attempts to route the call without waiting to match more digits. As a result, international and any other variable length calls do not route correctly.

Because you can configure translation patterns as non-urgent in Cisco Unified Communications Manager, you can configure similar translation patterns in the same partition and ensure that digit analysis can accurately match the patterns. Even if digit analysis identifies a match with a translation pattern, Cisco Unified Communications Manager attempts to match more digits in other translation patterns if you configure the translation pattern as non-urgent.

To route international and variable length calls correctly, make sure that you configure the translation patterns as non-urgent.

In Cisco Unified Communications Manager Administration, you can configure any translation pattern as urgent priority or non-urgent priority. The Urgent Priority check box displays in the Translation Pattern Configuration (Call Routing > Translation Pattern) and Intercom Translation Pattern Configuration (Call Routing > Intercom > Intercom Translation Pattern) windows. If you do not check this check box and if the dial plan contains overlapping patterns, Cisco Unified Communications Manager does not route the call until the interdigit timer expires (even if it is possible to dial a sequence of digits to choose a current match). To interrupt interdigit timing when Cisco Unified Communications Manager must route a call immediately, check this check box.

After you install or upgrade Cisco Unified Communications Manager, the Urgent Priority check box in translation patterns displays as checked and enabled. Update your translation patterns, if necessary, to accommodate your dial plan.

**Static digit analysis**

Static digit analysis (DA) ensures that whether a phone is registered or not, the device remains in the DA table, and the directory number intercepts the call.

**Configuration Tip**

Cisco Unified Communications Manager Assistant does not use translation patterns for failover. Instead, set up Call Forward No Answer (CFNA) with the data that was in the translation pattern for all Unified CM Assistant failed route points, and these route points must be removed.

The digit analysis process builds a static digit analysis engine with the patterns that are configured in the database during system initialization. This digit analysis engine reduces the propagation of patterns within a cluster of Cisco Unified Communications Managers and makes Cisco Unified Communications Manager more scalable.

In previous releases, the individual device control process read pattern information from the database and dynamically registered the patterns to the digit analysis process to build its digit analysis engine. Each pattern
had a mapping to its control process ID in the digit analysis engine. The control process ID of a pattern got changed dynamically if its associated device was reset or if a Cisco Unified Communications Manager server restarted. If a change to the control process ID took place, the digit analysis engine had to be changed dynamically, and its contents required propagation to other Cisco Unified Communications Manager servers. During call processing, the digit analysis engine returned the control process ID of a matched pattern.

The digit analysis process reads the pattern information directly from the database to build the static digit analysis engine during Cisco Unified Communications Manager initialization. With the static digit analysis engine, each pattern has a mapping to its callable endpoint name, which is a NumPlanPkID of the pattern in the database, a unique identifier to a configured pattern in Cisco Unified Communications Manager. The static digit analysis engine no longer holds the control process ID of a pattern.

Static digit analysis integrates with the changes to the device manager to support all existing functions and features. The device manager includes a table where a NumPlanPkID shows a one-to-one mapping to the control process ID of a pattern. When processing a call, digit analysis asks the device manager to get the control process ID for a matched pattern.

**Feature Description**

Cisco Unified Communications Manager includes these pattern types: Call Park, Call Forward, Meet-Me Conference, Device, Translation, Call Pickup Group, Route, and Message Waiting. The Device, Translation, and Route pattern types represent static patterns. The digit analysis process reads these patterns directly and inserts them into the static digit analysis engine during the initialization of a Cisco Unified Communications Manager. Other pattern types (Call Park, Call Forward, Meet-Me Conference, Call Pickup Group, and Message Waiting), which are intercept patterns, remain dynamic patterns. Their individual control process reads the pattern information from the database and then asks the digit analysis process to insert the pattern into the static digit analysis engine via registration messages.

All static patterns remain unchanged until their records are changed in the database. Static patterns do not require propagation because the database change notification is broadcast to the servers within a cluster. Dynamic patterns still use the existing propagating and updating mechanism to update the static digit analysis engines.

Regardless of its pattern type, each static pattern in the static digit analysis engine has a mapping to its PkID in the NumPlan table in the database. When a device registers its patterns to the device manager, the same PkID gets saved and mapped to its control process ID in the device manager. A new interface between the digit analysis and device manager retrieves the control process ID when a matched pattern is found in the static digit analysis engine during call processing.

**Caveat 1**

A potential loss of change notification exists in the current Cisco Unified Communications Manager release. This loss could cause a device that is registered with Cisco Unified Communications Manager to become unreachable by other devices. The following paragraphs provide troubleshooting for this potential problem.

The most common cause for this problem occurs when the DN that is assigned to the device belongs to a partition that is not contained in the calling search space of other devices. If the calling search space of other devices does contain the partition for that DN, other reasons may apply. For example, the DN changed only for that device, and the change notification from the database to Cisco Unified Communications Manager was lost. Resetting the device may not resolve the problem.

To resolve this problem, remove the DN and add the DN to the system again. Remove the DN from its device on the Directory Number Configuration window and on the Route Plan Report window. After you remove the DN, add it back in with the same partition, pattern, and other configuration information. The process should resolve the problem after you add the new DN to Cisco Unified Communications Manager again.
The same workaround applies to route patterns and translation patterns if similar problems exist.

Tip
Be sure to document all configurations before removing the patterns.

Caveat 2
Static digit analysis disables the configuration of several applications. These applications rely on the provision of duplicate patterns in the same calling search space. For example, the CTI application may be pattern 5000 in partition A, and a particular phone may be pattern 5000 in partition B. In previous releases, if the CTI route point is down, the phone will ring. With static digit analysis, however, the caller receives a busy tone. This limitation implies that the application failure does not get handled.

Administrators would normally use Call Forward No Answer and Call Forward on failure to handle application failure, but when the pattern on the CTI route point is 5XXX, you cannot configure a forward destination of 5XXX. To resolve this limitation, you can now perform configuration of X characters in Call Forward destinations.

The following example demonstrates the functionality of digit analysis for the Cisco Unified Communications Manager Assistant application.

Cisco Unified Communications Manager Assistant Example with Static Digit Analysis
You must make the following modification: configure 1xxx as a CFNA mask and CSS-E as a CFNA calling search space for the CTI route point to handle the CTI route point failure case.

When static digit analysis gets used, the following processing takes place:

• If the CTI route point (RP) is up, 1000/IPMA:EveryOne calls 1001. The call routes through CTI route point IPMA/1XXX. (Routing does not change from previous releases.)

• If the CTI route point is down, 1000/IPMA:EveryOne calls 1001. The call goes to the CTI route point, and its CFNA is triggered. The forwarding feature routes the call through the translation pattern Everyone/1xxx, and the call reaches Manager/1001 after translation.

Without configuring the CFNA in the CTI route point, the translation pattern never gets matched, and the Cisco Unified Communications Manager Assistant application fails.

Calling party normalization
In line with E.164 standards, calling party normalization, which adds the support of international escape character, +, to Cisco Unified Communications Manager, enhances the dialing capabilities of some phones and improves call back functionality when a call is routed to multiple geographical locations; that is, the feature ensures that the called party can return a call without having to modify the directory number in the call log directories on the phone. Additionally, calling party normalization allows you to globalize and localize phone numbers, so the appropriate calling number presentation displays on the phone.

Tip
Configuring calling party normalization alleviates issues with toll bypass where the call is routed to multiple locations over the IP WAN. In addition, it allows Cisco Unified Communications Manager to distinguish the origin of the call to globalize or localize the calling party number for the phone user.
For information on the international escape character, +, see the Use the international escape character, on page 161.

**Special characters and settings**

Cisco Unified Communications Manager Administration allows you to use special characters and settings to perform the following tasks:

- Allowing a single route pattern or hunt pilot to match a range of numbers
- Removing a portion of the dialed digit string
- Manipulating the appearance of the calling party number for outgoing calls
- Manipulating the dialed digits, or called party number, for outgoing calls

**Related Topics**

- Caller Identification support with device control protocols in Cisco Unified Communications Manager, on page 188
- Called party number transformations settings, on page 181

**Use the international escape character**

Configuring the international escape character, +, in Cisco Unified Communications Manager Administration allows your phone users to place calls without having to remember and enter the international direct dialing prefix/international escape code that is associated with the called party. Depending on the phone model, for example, dual-mode phones, your phone users can dial + on the keypad of the phone. In other cases, the phone user can return calls by accessing the call log directory entries that contain +. In addition, using the international escape character allows you to support globalization of calling party numbers, which is part of the calling party normalization feature; for information on the calling party normalization feature, see the Cisco Unified Communications Manager Features and Services Guide.

The international escape character, +, signifies the international access code in a complete E.164 number format. For example, NANP numbers have an E.164 global format in the format +1 214 555 1234. The + is a leading character that gets replaced by service providers in different countries with the international access code to achieve global dial plans.

In cases where you define a pattern with a dialable + digit in Cisco Unified Communications Manager Administration, a plus sign preceded by a backslash, that is, \+, indicates that you want to configure the international escape character +. In other cases in Cisco Unified Communications Manager Administration, for example, in prefix or mask fields, you can enter + to indicate the international escape character.

See the following sections for more information on the international escape character, +:

**Configuring \+ for the International Escape Character +**

To configure the international escape character, +, for patterns and directory numbers, you configure \+ in the windows in the following table:
Table 13: Entering \+ in Cisco Unified Communications Manager Administration

<table>
<thead>
<tr>
<th>Configuration Window</th>
<th>Fields that Support Entering + for International Escape Character</th>
</tr>
</thead>
<tbody>
<tr>
<td>Route Pattern, Hunt Pilot, and Translation Pattern</td>
<td>Route Pattern, Hunt Pilot, and Translation Pattern</td>
</tr>
<tr>
<td>Directory Number</td>
<td>Directory Number</td>
</tr>
<tr>
<td>Intercom Translation Pattern</td>
<td>Intercom Translation Pattern</td>
</tr>
<tr>
<td>Calling Party Transformation</td>
<td>Pattern</td>
</tr>
<tr>
<td>Called Party Transformation</td>
<td>Pattern</td>
</tr>
</tbody>
</table>

Entering + in the windows in the previous table does not configure the international escape character; instead, entering the + in the pattern fields means that the system should match one or more of the previous characters during digit analysis. Consider the following information for configuring the international escape character in the windows in the previous table:

- To configure the international escape character for supported patterns, make sure that you enter \+ in the pattern or Directory Number field.
- For all patterns in the previous table except for the directory number, you can configure the international escape character, \+, at the beginning, in the middle, or at the end of a pattern. For example, you can configure \+91! or 0\+23! in the pattern fields. For directory numbers, you can configure the international escape character, \+, at the beginning of the number only.
- You can configure \+ as a dialable character and a + wildcard within a single pattern; for example, you can configure a pattern like 1234\+56+, where \+ equals the dialable character and + serves as the wildcard.
- You can configure multiple international escape characters \+ in a single pattern; for example, you can configure a pattern like 147\+56\+89\+.

Meet-Me patterns, Call Park (and related call park features; for example, Directed Call Park) patterns, and Call Pickup patterns do not support the international escape character, +, so you cannot enter \+ in the pattern fields that are configured for these features.

Tip

Configuring + for the International Escape Character

The following table provides the configuration windows and fields where you can enter + to indicate the international escape character +.
## Table 14: Configuring + for the International Escape Character in Cisco Unified Communications Manager Administration

<table>
<thead>
<tr>
<th>Configuration Window</th>
<th>Fields that Support Entering + for International Escape Character</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Pool</td>
<td>Incoming Calling Party Settings (Prefix fields for Unknown, Subscriber, International Number, National Number)</td>
</tr>
<tr>
<td></td>
<td>Incoming Called Party Settings (Prefix fields for Unknown, Subscriber, International Number, National Number)</td>
</tr>
<tr>
<td>Service Parameter</td>
<td>all Incoming Calling Party prefix service parameters and Incoming Called Party service parameters for H.323</td>
</tr>
<tr>
<td>Route Pattern, Hunt Pilot, Intercom</td>
<td>Calling Party Transform Mask, Called Party Transform Mask, and Prefix Digits (Outgoing Calls)</td>
</tr>
<tr>
<td>Translation Pattern, and Translation Pattern</td>
<td></td>
</tr>
<tr>
<td>Directory Number</td>
<td>External Phone Number Mask and all Call Forwarding fields</td>
</tr>
<tr>
<td>Calling Party Transformation</td>
<td>Calling Party Transform Mask and Prefix Digits (Outgoing Calls)</td>
</tr>
<tr>
<td>Called Party Transformation</td>
<td>Called Party Transform Mask and Prefix Digits</td>
</tr>
<tr>
<td>Voice Mail Port and Voice Mail Port Wizard</td>
<td>External Number Mask</td>
</tr>
<tr>
<td>Message Waiting</td>
<td>Message Waiting Number</td>
</tr>
<tr>
<td>Voice Mail Pilot</td>
<td>Voice Mail Pilot Number</td>
</tr>
<tr>
<td>Gateway</td>
<td>Incoming Calling Party Settings (Prefix fields for Unknown, Subscriber, International Number, National Number)</td>
</tr>
<tr>
<td></td>
<td>Incoming Called Party Settings (Prefix fields for Unknown, Subscriber, International Number, National Number) H.323 gateways</td>
</tr>
<tr>
<td></td>
<td>Caller ID DN, and Prefix DN</td>
</tr>
<tr>
<td><strong>Tip</strong></td>
<td>MGCP gateways support sending the international escape character + ; H.323 gateways do not support the +, so the gateway strips the + when a calling or called party offers it to the gateway.</td>
</tr>
<tr>
<td>Trunk</td>
<td>Incoming Calling Party Settings (Prefix fields for Unknown, Subscriber, International Number, National Number) H.323 trunks</td>
</tr>
<tr>
<td></td>
<td>Caller ID DN and Prefix DN</td>
</tr>
<tr>
<td>Speed Dial and Abbreviated Dial</td>
<td>Number (allows the international escape character, +, to display as part of the speed dial number on the phone)</td>
</tr>
</tbody>
</table>
Gateways and Trunks that Support International Escape Character +

SIP and MGCP gateways can support sending the international escape character, +, for calls. H.323 gateways do not support the +. QSIG trunks do not attempt to send the +, but SIP trunks can support sending the +.

For outgoing calls through a gateway that supports +, Cisco Unified Communications Manager can send the + with the dialed digits to the gateway. For outgoing calls through a gateway that does not support +, the gateway strips the + when Cisco Unified Communications Manager sends the call information to the gateway.

When + is not supported but the global calling party number includes +, configure the called party transformations and route patterns to send the outdial digits in a format that the device supports.

If you want to do so, you can configure the Strip + on Outbound Calls service parameter, which supports the Cisco CallManager service. This parameter determines whether Cisco Unified Communications Manager strips the international escape character, +, from the calling and called parties for outgoing calls through MGCP gateways and SIP trunks. If your network or far-end gateway does not recognize the + as a digit, set this parameter to False; if you set this parameter to True and the + is not supported in network or by the receiving gateway, calls that use + may drop. Ensure that calls over QSIG trunks do not utilize + because QSIG does not send the +. This parameter does not impact H.323 outbound calls because H.323 gateways unconditionally strip the + when they route outbound calls.

If you set the Strip + on Outbound Calls service parameter to True, Cisco Unified Communications Manager strips the + for the calling and called parties for all outgoing calls through all MGCP gateways and SIP trunks. To ensure that Cisco Unified Communications Manager does not strip the + for outgoing calls through particular MGCP gateways and SIP trunks, configure the calling party and called party transformation patterns for outgoing gateways to include the + prefix for international calls.

The H.323 protocol does not support the international escape character, +. To ensure that correct prefixes, including the international escape character, +, get applied for inbound calls over H.323 gateways/trunks, you must configure the incoming called party settings in the service parameter, device pool, H.323 gateway, or H.323 trunk windows; that is, configuring the incoming called party settings ensures that when a inbound call comes from a H.323 gateway or trunk, Cisco Unified Communications Manager transforms the called party number back to the value that was originally sent over the trunk/gateway.

For example, to ensure that the correct DN patterns get used with SAF/call control discovery for inbound calls over H.323 gateways/trunks, you must configure the incoming called party settings in the service parameter, device pool, or H.323 (non-gatekeeper controlled) trunk window. See the following example for more information.

- A caller places a call to +19721230000 to Cisco Unified Communications Manager A.
- Cisco Unified Communications Manager A receives +19721230000 and transforms the number to 55519721230000 before sending the call to the H.323 trunk. In this case, your configuration indicates that the international escape character + should be stripped and 555 should be prepended for calls of International type.
- For this inbound call from the trunk, Cisco Unified Communications Manager B receives 55519721230000 and transforms the number back to +19721230000 so that digit analysis can use the value as it was sent by the caller. In this case, your configuration for the incoming called party settings indicates that you want 555 to be stripped and +1 to be prepended to called party numbers of International type.
The service parameters support the Cisco CallManager service. To configure the service parameters, click Advanced in the Service Parameter Configuration window for the Cisco CallManager service; then, locate the H.323 pane for the following parameters:

- Incoming Called Party National Number Prefix - H.323
- Incoming Called Party International Number Prefix - H.323
- Incoming Called Party Subscriber Number Prefix - H.323
- Incoming Called Party Unknown Number Prefix - H.323

These service parameters allow you to prefix digits to the called number based on the Type of Number field for the inbound offered call. You can also strip a specific number of leading digits before the prefix gets applied. To prefix and strip digits by configuring these parameter fields, use the following formula, x:y, where x represents the exact prefix that you want to add to called number and y represents the number of digits stripped; be aware that the colon separates the prefix and the number of stripped digits. For example, enter 91010:6 in the field, which means that you want to strip 6 digits and then add 901010 to the beginning of the called number. In this example, a national call of 2145551234 becomes 910101234. You can strip up to 24 digits and prefix/add up to than 16 digits.

**Phones that Support International Escape Character +**

The following Cisco Unified IP Phones, which run SIP or SCCP unless noted otherwise, can display + on the phone screen, speed dials, directory numbers, and in call log (Redial, Missed Calls, and so on) directories on the phone.

- 7906 and 7911
- 7921 (SCCP only) and 7931
- 7941, 7942, 7945
- 7961, 7965
- 7970, 7971, 7975
- 7985 (SCCP only)

The Nokia S60, a dual-mode phone, also supports + dialing from the keypad on the phone. For example, a caller in the United States calls an international number in India. If the caller uses a dual-mode phone, the caller can directly dial + to represent the international number. The caller may call 0+91802501523 or +918025010523, depending on the outgoing route pattern settings. Dialing the + on the keypad assumes that the outgoing gateway can support the +; if the outgoing gateway does not support +, you must configure the route pattern like \+!, where Cisco Unified Communications Manager strips the \+ and prefixes 011 to transform the international number to 011 91 8025010523.

Consider the following information about + and the phone:

- If a phone displays the + in a call log directory entry on the phone, the end user can place a call without having to edit the entry in the call log directory. If the outgoing gateway does not support the +, configure the outgoing route pattern so that Cisco Unified Communications Manager can strip the international escape code and prefix the international access code to the directory number in the call log directory.

- If you do not configure transformation patterns to localize the calling party number, a called party may receive an international call that contains + in the calling party number, for example, 0+494692022002 or +4940692022002, depending on the configuration of the incoming gateway. If the called party does
not answer the call, the calling party number gets stored with the + in the call log directories on the phone. The called party can return the call without having to edit the entry in the call log directory.

• A caller can place a call to a speed dial number that is configured as an E.164 number that contains the +.

• Cisco Unified IP Phones 7902, 7905, 7912, 7920, 7940, and 7960 that run SCCP can receive calls from directory numbers that contain the international escape character, +, although these phones do not display the + on the phone because Cisco Unified Communications Manager strips the + before the call completes.

• SRST does not work for phones that are running SIP that display the + in the call alerting pane or the call log directories on the phone; therefore, phones that are running SIP that display the + cannot register with SRST-enabled gateways, and calls to the SRST-enabled gateway fail if a directory number that is used for the call includes the +. SCCP phones that display the + on the phone can register with SRST.

Related Topics

Calling Party Normalization, on page 521
Device pools, on page 45
Wildcards and special characters in route patterns and hunt pilots, on page 166

Wildcards and special characters in route patterns and hunt pilots

Wildcards and special characters in route patterns and hunt pilots allow a single route pattern or hunt pilot to match a range of numbers (addresses). Use these wildcards and special characters also to build instructions that enable the Cisco Unified Communications Manager to manipulate a number before sending it to an adjacent system.

The following table describes the wildcards and special characters that Cisco Unified Communications Manager supports.

Table 15: Wildcards and Special Characters

<table>
<thead>
<tr>
<th>Character</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
</table>
| @         | The at symbol (@) wildcard matches all National Numbering Plan numbers. Each route pattern can have only one @ wildcard. | The route pattern 9.@ routes or blocks all numbers that the National Numbering Plan recognizes. The following route patterns examples show National Numbering Plan numbers that the @ wildcard encompasses:
  • 0
  • 1411
  • 19725551234
  • 101028819725551234
  • 01133123456789 |
<p>| X         | The X wildcard matches any single digit in the range 0 through 9. | The route pattern 9XXX routes or blocks all numbers in the range 9000 through 9999. |</p>
<table>
<thead>
<tr>
<th>Character</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>!</td>
<td>The exclamation point (!) wildcard matches one or more digits in the range 0 through 9.</td>
<td>The route pattern 9! routes or blocks all numbers in the range 910 through 91999999999999999999999.</td>
</tr>
<tr>
<td>?</td>
<td>The question mark (?) wildcard matches zero or more occurrences of the preceding digit or wildcard value.</td>
<td>The route pattern 91X? routes or blocks all numbers in the range 91 through 91999999999999999999999.</td>
</tr>
<tr>
<td>+</td>
<td>The plus sign (+) wildcard matches one or more occurrences of the preceding digit or wildcard value.</td>
<td>The route pattern 91X+ routes or blocks all numbers in the range 910 through 91999999999999999999999.</td>
</tr>
<tr>
<td>[ ]</td>
<td>The square bracket ([ ]) characters enclose a range of values.</td>
<td>The route pattern 813510[012345] routes or blocks all numbers in the range 8135100 through 8135105.</td>
</tr>
<tr>
<td>-</td>
<td>The hyphen (-) character, used with the square brackets, denotes a range of values.</td>
<td>The route pattern 813510[0-5] routes or blocks all numbers in the range 8135100 through 8135105.</td>
</tr>
<tr>
<td>^</td>
<td>The circumflex (^) character, used with the square brackets, negates a range of values. Ensure that it is the first character following the opening bracket ([). Each route pattern can have only one ^ character.</td>
<td>The route pattern 813510[^0-5] routes or blocks all numbers in the range 8135106 through 8135109.</td>
</tr>
<tr>
<td>.</td>
<td>The dot (.) character, used as a delimiter, separates the Cisco Unified Communications Manager access code from the directory number. Use this special character, with the discard digits instructions, to strip off the Cisco Unified Communications Manager access code before sending the number to an adjacent system. Each route pattern can have only one dot (.) character.</td>
<td>The route pattern 9.@ identifies the initial 9 as the Cisco Unified Communications Manager access code in a National Numbering Plan call.</td>
</tr>
<tr>
<td>*</td>
<td>The asterisk (*) character can provide an extra digit for special dialed numbers.</td>
<td>You can configure the route pattern *411 to provide access to the internal operator for directory assistance.</td>
</tr>
<tr>
<td>#</td>
<td>The octothorpe (#) character generally identifies the end of the dialing sequence. Ensure the # character is the last character in the pattern.</td>
<td>The route pattern 901181910555# routes or blocks an international number that is dialed from within the National Numbering Plan. The # character after the last 5 identifies this digit as the last digit in the sequence.</td>
</tr>
</tbody>
</table>
Examples

For examples, see the Use the international escape character, on page 161.

The following table lists Cisco Unified Communications Manager Administration fields that require route patterns or hunt pilots and shows the valid entries for each field.

**Table 16: Field Entries**

<table>
<thead>
<tr>
<th>Field</th>
<th>Valid entries</th>
</tr>
</thead>
<tbody>
<tr>
<td>Call Park Number/Range</td>
<td>[ ^0123456789 - ] X*#</td>
</tr>
<tr>
<td>Calling Party Transform Mask</td>
<td>0123456789 X A B C D *# +</td>
</tr>
<tr>
<td>Called Party Transform Mask</td>
<td>0123456789 X A B C D *# +</td>
</tr>
<tr>
<td>Caller ID DN (Gateways and Trunks)</td>
<td>0123456789 X*# +</td>
</tr>
<tr>
<td>Directory Number</td>
<td>+[ ^0123456789 - ] +? X*# +</td>
</tr>
<tr>
<td>Directory Number (Call Pickup Group Number)</td>
<td>0123456789</td>
</tr>
<tr>
<td>External Phone Number Mask</td>
<td>0123456789 X*# +</td>
</tr>
<tr>
<td>Forward All</td>
<td>0123456789*# +</td>
</tr>
<tr>
<td>Forward Busy</td>
<td>0123456789*# +</td>
</tr>
<tr>
<td>Forward No Answer</td>
<td>0123456789*# +</td>
</tr>
<tr>
<td>Meet-Me Conference Number</td>
<td>[ ^0123456789 - ] X*#</td>
</tr>
<tr>
<td>Prefix Digits</td>
<td>0123456789 A B C D *# +</td>
</tr>
<tr>
<td>Prefix DN (Gateways and Trunks)</td>
<td>0123456789*# +</td>
</tr>
<tr>
<td>Route Filter Tag Values</td>
<td>[ ^0123456789 - ] X*#</td>
</tr>
<tr>
<td>Route Pattern</td>
<td>[ ^0123456789 A B C D - ] +?! X*# + .@+</td>
</tr>
<tr>
<td>Translation Pattern</td>
<td>[ ^0123456789 A B C D - ] +?! X*# + .@+</td>
</tr>
</tbody>
</table>
Discard digits instructions

A discard digits instruction (DDI) removes a portion of the dialed digit string before passing the number on to the adjacent system. A DDI must remove portions of the digit string, for example, when an external access code is needed to route the call to the PSTN, but the PSTN switch does not expect that access code.

The following table lists DDIs and describes the effects of applying each DDI to a dialed number.

### Table 17: Discard Digits Instructions

<table>
<thead>
<tr>
<th>DDI</th>
<th>Effect</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>10-10-Dialing</td>
<td>This DDI removes • IXC access code</td>
<td>Route pattern: 9.@&lt;br&gt;Dialed digit string: 910102889728135000&lt;br&gt;After applying DDI: 99728135000</td>
</tr>
<tr>
<td>10-10-Dialing Trailing-#</td>
<td>This DDI removes • IXC access code &lt;br&gt;• End-of-dialing character for international calls</td>
<td>Route pattern: 9.@&lt;br&gt;Dialed digit string: 9101028801181910555#&lt;br&gt;After applying DDI: 901181910555</td>
</tr>
<tr>
<td>11/10D-&gt;7D</td>
<td>This DDI removes • Long-distance direct-dialing code &lt;br&gt;• Long-distance operator-assisted dialing code &lt;br&gt;• IXC access code &lt;br&gt;• Area code &lt;br&gt;• Local area code &lt;br&gt;This DDI creates a 7-digit local number from an 11- or 10-digit dialed number.</td>
<td>Route pattern: 9.@&lt;br&gt;Dialed digit string: 919728135000 or 99728135000&lt;br&gt;After applying DDI: 98135000</td>
</tr>
</tbody>
</table>

Related Topics

Use the international escape character, on page 161
<table>
<thead>
<tr>
<th>DDI</th>
<th>Effect</th>
<th>Example</th>
</tr>
</thead>
</table>
| 11/10D->7D Trailing-# | This DDI removes  
• Long-distance direct-dialing code  
• Long-distance operator-assisted dialing code  
• IXC access code  
• Area code  
• Local area code  
• End-of-dialing character for international calls  
This DDI creates a 7-digit local number from an 11- or 10-digit dialed number. | Route pattern: 9.@  
Dailed digit string: 919728135000  
or 99728135000  
After applying DDI: 98135000 |
| 11D->10D | This DDI removes  
• Long-distance direct-dialing code  
• Long-distance operator-assisted dialing code  
• IXC access code | Route pattern: 9.@  
Dailed digit string: 919728135000  
After applying DDI: 99728135000 |
| 11D->10D Trailing-# | This DDI removes  
• Long-distance direct-dialing code  
• Long-distance operator-assisted dialing code  
• End-of-dialing character for international calls  
• IXC access code | Route pattern: 9.@  
Dailed digit string: 919728135000  
After applying DDI: 99728135000 |
| Intl TollBypass | This DDI removes  
• International access code  
• International direct-dialing code  
• Country code  
• IXC access code  
• International operator-assisted dialing code | Route pattern: 9.@  
Dailed digit string: 901181910555  
After applying DDI: 9910555 |
<table>
<thead>
<tr>
<th>DDI</th>
<th>Effect</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intl TollBypass Trailing-#</td>
<td>This DDI removes</td>
<td>Route pattern: 9.@</td>
</tr>
<tr>
<td></td>
<td>• International access code</td>
<td>Dialed digit string: 901181910555#</td>
</tr>
<tr>
<td></td>
<td>• International direct-dialing code</td>
<td>After applying DDI: 9910555</td>
</tr>
<tr>
<td></td>
<td>• Country code</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• IXC access code</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• International operator-assisted dialing code</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• End-of-dialing character</td>
<td></td>
</tr>
<tr>
<td>NoDigits</td>
<td>This DDI removes no digits.</td>
<td>Route pattern: 9.@</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Dialed digit string: 919728135000</td>
</tr>
<tr>
<td></td>
<td></td>
<td>After applying DDI: 91972813500</td>
</tr>
<tr>
<td>Trailing-#</td>
<td>This DDI removes</td>
<td>Route pattern: 9.@</td>
</tr>
<tr>
<td></td>
<td>• End-of-dialing character for international calls</td>
<td>Dialed digit string: 901181910555#</td>
</tr>
<tr>
<td></td>
<td></td>
<td>After applying DDI: 901181910555</td>
</tr>
<tr>
<td>PreAt</td>
<td>This DDI removes all digits prior to the National Numbering Plan portion of the route pattern, including</td>
<td>Route pattern: 8.9@</td>
</tr>
<tr>
<td></td>
<td>• Cisco Unified Communications Manager external access code</td>
<td>Dialed digit string: 89972813500</td>
</tr>
<tr>
<td></td>
<td>• PBX external access code</td>
<td>After applying DDI: 972813500</td>
</tr>
<tr>
<td>PreAt Trailing-#</td>
<td>This DDI removes all digits prior to the National Numbering Plan portion of the route pattern, including</td>
<td>Route pattern: 8.9@</td>
</tr>
<tr>
<td></td>
<td>• Cisco Unified Communications Manager external access code</td>
<td>Dialed digit string: 8901181910555#</td>
</tr>
<tr>
<td></td>
<td>• PBX external access code</td>
<td>After applying DDI: 01181910555</td>
</tr>
<tr>
<td></td>
<td>• End-of-dialing character for international calls</td>
<td></td>
</tr>
<tr>
<td>DDI</td>
<td>Effect</td>
<td>Example</td>
</tr>
<tr>
<td>---------------------</td>
<td>--------------------------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| PreAt 10-10-Dialing | This DDI removes all digits prior to the National Numbering Plan portion of the route pattern, including - Cisco Unified Communications Manager external access code - PBX external access code - IXC access code | Route pattern: 8.9@  
Dailed digit string: 8910289728135000  
After applying DDI: 9728135000 |
| PreAt 10-10-Dialing Trailing-# | This DDI removes all digits prior to the National Numbering Plan portion of the route pattern, including - Cisco Unified Communications Manager external access code - PBX external access code - IXC access code - End-of-dialing character for international calls | Route pattern: 8.9@  
Dailed digit string: 891012801181910555#  
After applying DDI: 01181910555 |
| PreAt 11/10D->7D    | This DDI removes all digits prior to the National Numbering Plan portion of the route pattern, including - Cisco Unified Communications Manager external access code - PBX external access code - Long-distance direct-dialing code - Long-distance operator-assisted dialing code - IXC access code - Area code - Local area code  
This DDI creates a 7-digit local number from an 11- or 10-digit dialed number. | Route pattern: 8.9@  
Dailed digit string: 8919728135000  
or 899728135000  
After applying DDI: 8135000 |
### DDI

<table>
<thead>
<tr>
<th>DDI</th>
<th>Effect</th>
<th>Example</th>
</tr>
</thead>
</table>
| PreAt 11/10D->7D Trailing-# | This DDI removes all digits prior to the National Numbering Plan portion of the route pattern, including  
- Cisco Unified Communications Manager external access code  
- PBX external access code  
- Long-distance direct-dialing code  
- Long-distance operator-assisted dialing code  
- IXC access code  
- Area code  
- Local area code  
- End-of-dialing character for international calls  
This DDI creates a 7-digit local number from an 11- or 10-digit dialed number. | Route pattern: 8.9@  
Dialed digit string: 8919728135000  
or 899728135000  
After applying DDI: 8135000 |
| PreAt 11D->10D | This DDI removes all digits prior to the National Numbering Plan portion of the route pattern, including  
- Cisco Unified Communications Manager external access code  
- PBX external access code  
- Long-distance direct-dialing code  
- Long-distance operator-assisted dialing code  
- IXC access code  
Route pattern: 8.9@  
Dialed digit string: 8919728135000  
After applying DDI: 9728135000 |
<table>
<thead>
<tr>
<th>DDI</th>
<th>Effect</th>
<th>Example</th>
</tr>
</thead>
</table>
| PreAt 11D->10D Trailing-#    | This DDI removes all digits prior to the National Numbering Plan portion of the route pattern, including  
|                              | • Cisco Unified Communications Manager external access code  
|                              | • PBX external access code  
|                              | • Long-distance direct-dialing code  
|                              | • Long-distance operator-assisted dialing code  
|                              | • IXC access code  
|                              | • End-of-dialing character for international calls                                                                                                                                                    | Route pattern: 8.9@  
|                              | Dialed digit string: 891972813500  
|                              | After applying DDI: 972813500                                                                                                                                                                          |
| PreAt Intl TollBypass        | This DDI removes all digits prior to the National Numbering Plan portion of the route pattern, including  
|                              | • Cisco Unified Communications Manager external access code  
|                              | • PBX external access code  
|                              | • International access code  
|                              | • International direct-dialing code  
|                              | • Country code  
|                              | • IXC access code  
|                              | • International operator-assisted dialing code  
|                              |                                                                                                                                                    | Route pattern: 8.9@  
|                              | Dialed digit string: 8901181910555  
<p>|                              | After applying DDI: 910555                                                                                                                                                                          |</p>
<table>
<thead>
<tr>
<th>DDI</th>
<th>Effect</th>
<th>Example</th>
</tr>
</thead>
</table>
| PreAt Intl TollBypass        | This DDI removes all digits prior to the National Numbering Plan portion of the route pattern, including | Route pattern: 8.9@  
Dialled digit string: 8901181910555#  
After applying DDI: 910555 |
| Trailing-#                  | • Cisco Unified Communications Manager external access code  
• PBX external access code  
• International access code  
• International direct-dialing code  
• Country code  
• IXC access code  
• International operator-assisted dialing code  
• End-of-dialing character |                                                                                   |
| PreDot                      | This DDI removes  
• Cisco Unified Communications Manager external access code | Route pattern: 8.9@  
Dialled digit string: 899728135000  
After applying DDI: 99728135000 |
| PreDot Trailing-#            | This DDI removes  
• Cisco Unified Communications Manager external access code  
• End-of-dialing character for international calls | Route pattern: 8.9@  
Dialled digit string: 8901181910555#  
After applying DDI: 901181910555 |
| PreDot 10-10-Dialing         | This DDI removes  
• Cisco Unified Communications Manager external access code  
• IXC access code | Route pattern: 8.9@  
Dialled digit string: 89101028801181910555#  
After applying DDI: 99728135000 |
| PreDot 10-10-Dialing         | This DDI removes  
• Cisco Unified Communications Manager external access code  
• IXC access code  
• End-of-dialing character for international calls | Route pattern: 8.9@  
Dialled digit string: 89101028801181910555#  
After applying DDI: 901181910555 |
<table>
<thead>
<tr>
<th>DDI</th>
<th>Effect</th>
<th>Example</th>
</tr>
</thead>
</table>
| PreDot 11/10D→7D        | This DDI removes                                                       | Route pattern: 8.9@
|                         | • Cisco Unified Communications Manager external access code           | Dialed digit string: 8919728135000 or 899728135000
|                         | • Long-distance direct-dialing code                                   | After applying DDI: 98135000                                           |
|                         | • Long-distance operator-assisted dialing code                         |                                                                         |
|                         | • IXC access code                                                      |                                                                         |
|                         | • Area code                                                            |                                                                         |
|                         | • Local area code                                                      |                                                                         |
|                         | This DDI creates a 7-digit local number from an 11- or 10-digit dialed number. |                                                                         |
| PreDot 11/10D→7D Trailing-# | This DDI removes                                                       | Route pattern: 8.9@
|                         | • Cisco Unified Communications Manager external access code           | Dialed digit string: 8919728135000 or 899728135000
|                         | • Long-distance direct-dialing code                                   | After applying DDI: 98135000                                           |
|                         | • Long-distance operator-assisted dialing code                         |                                                                         |
|                         | • IXC access code                                                      |                                                                         |
|                         | • Area code                                                            |                                                                         |
|                         | • Local area code                                                      |                                                                         |
|                         | • End-of-dialing character for international calls                    |                                                                         |
|                         | This DDI creates a 7-digit local number from an 11- or 10-digit dialed number. |                                                                         |
| PreDot 11D→10D          | This DDI removes                                                       | Route pattern: 8.9@
|                         | • Cisco Unified Communications Manager external access code           | Dialed digit string: 8919728135000 or 899728135000
|                         | • Long-distance direct-dialing code                                   | After applying DDI: 99728135000                                        |
|                         | • Long-distance operator-assisted dialing code                         |                                                                         |
|                         | • IXC access code                                                      |                                                                         |
### Calling and Called party transformations

Cisco Unified Communications Manager Administration allows you to manipulate the calling party number and the called party number that Cisco Unified Communications Manager sends with each call setup message.

<table>
<thead>
<tr>
<th>DDI</th>
<th>Effect</th>
<th>Example</th>
</tr>
</thead>
</table>
| PreDot 11D->10D Trailing-# | This DDI removes  
• Cisco Unified Communications Manager external access code  
• Long-distance direct-dialing code  
• Long-distance operator-assisted dialing code  
• IXC access code  
• End-of-dialing character for international calls | Route pattern: 8.9@  
Dialled digit string: 891972813500  
After applying DDI: 99728135000 |
| PreDot Intl TollBypass | This DDI removes  
• Cisco Unified Communications Manager external access code  
• International access code  
• International direct-dialing code  
• Country code  
• IXC access code  
• International operator-assisted dialing code | Route pattern: 8.9@  
Dialled digit string: 8901181910555  
After applying DDI: 9910555 |
| PreDot Intl TollBypass Trailing-# | This DDI removes  
• Cisco Unified Communications Manager external access code  
• International access code  
• International direct-dialing code  
• Country code  
• IXC access code  
• International operator-assisted dialing code  
• End-of-dialing character | Route pattern: 8.9@  
Dialled digit string: 8901181910555#  
After applying DDI: 9910555 |
You configure calling and called party transformation patterns to provide context-sensitive modifications to a calling or called party; Cisco Unified Communications Manager does not use these patterns for routing calls.

Both calling party transformations and called party transformations can be used with the Cisco Intercompany Media Engine (Cisco IME). See the Cisco Intercompany Media Engine Installation and Configuration Guide for details.

Related Topics

Caller Identification support with device control protocols in Cisco Unified Communications Manager, on page 188

Calling party number transformations settings

Calling party transformations settings allow you to manipulate the appearance of the calling party number for outgoing calls. Cisco Unified Communications Manager uses the calling party number for calling line identification (CLID). During an outgoing call, the CLID passes to each private branch exchange (PBX), central office (CO), and interexchange carrier (IXC) as the call progresses. The called party receives the calling line identification (CLID) when the call is offered to the called party.

Configuration for calling party transformations settings that are used in route lists occurs in the individual route groups that comprise the list. The calling party transformations settings that are assigned to the route groups in a route list override any calling party transformations settings that are assigned to a route pattern that is associated with that route list.

You can set the following calling party transformation settings in the route group configuration:

- Use Calling Party's External Phone Number Mask
- Calling Party Transform Mask
- Prefix Digits (Outgoing Calls)
- Calling Party Number Type
- Calling Party Numbering Plan

Table 14-8 describes the fields, options, and values that are used to specify calling party number transformations.
Table 18: Calling Party Number Transformations Settings

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| Use Calling Party’s External Phone Number Mask | This field determines whether the full, external phone number is used for calling line identification (CLID) on outgoing calls. (Configure the external number by using the Directory Number Configuration window.)
You can set the following Calling Party Transformations settings for the route group by clicking the members in the Route List Details panel of the Route List Configuration window:
  • Default: This setting indicates that the route group does not govern the calling party external phone number and calling party transform masks. If a calling party external phone number mask or transform mask is chosen for the route pattern, calls that are routed through this route group use those masks.
  • Off: This setting indicates that the calling party external phone number is not used for CLID. If no transform mask is entered for this route group, calls that are routed through this group do not get associated with a CLID.
  • On: This setting indicates that the calling party full, external number is used for CLID.
The external phone number mask can contain up to 24 digits. |
| Calling Party Transform Mask                   | This field specifies the calling party transform mask for all calls that are routed through this route group. Valid values for this field range from 0 through 9, the wildcard character X, and the characters *, #, and +. You can also leave this field blank. If it is blank and the preceding field is set to Off, this means that no calling party number is available for CLID.
The calling party transform mask can contain up to 50 digits. |
| Prefix Digits (Outgoing Calls)                 | This field contains a prefix digit or a set of Prefix Digits (Outgoing Calls) that are appended to the calling party number on all calls that are routed through this route group. Valid values for this field range from 0 through 9, the characters *, #, and +, and blank. Prefix Digits (Outgoing Calls) can contain up to 50 digits on route patterns or up to 24 digits on DNs. |
| Calling Line ID Presentation                   | Cisco Unified Communications Manager uses calling line ID presentation (CLIP/CLIR) as a supplementary service to allow or restrict the originating caller phone number on a call-by-call basis.
Choose whether you want the Cisco Unified Communications Manager to allow or restrict the display of the calling party phone number on the called party phone display for this route pattern.
Choose Default if you do not want to change calling line ID presentation. Choose Allowed if you want Cisco Unified Communications Manager to allow the display of the calling number. Choose Restricted if you want Cisco Unified Communications Manager to block the display of the calling number. |
<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Calling Name Presentation</td>
<td>Cisco Unified Communications Manager uses calling name presentation (CNIP/CNIR) as a supplementary service to allow or restrict the originating caller name on a call-by-call basis. Choose whether you want the Cisco Unified Communications Manager to allow or restrict the display of the calling party name on the called party phone display for this route pattern. Choose Default if you do not want to change calling name presentation. Choose Allowed if you want Cisco Unified Communications Manager to display the calling name information. Choose Restricted if you want Cisco Unified Communications Manager to block the display of the calling name information.</td>
</tr>
</tbody>
</table>
| Calling Party Number Type         | Choose the format for the number type in calling party directory numbers. Cisco Unified Communications Manager sets the calling directory number (DN) type. Cisco recommends that you do not change the default value unless you have advanced experience with dialing plans such as NANP or the European dialing plan. You may need to change the default in Europe because Cisco Unified Communications Manager does not recognize European national dialing patterns. You can also change this setting when you are connecting to a PBX that expects the calling directory number to be encoded to a non-national type numbering plan. Choose one of the following options:  
  • Cisco Unified Communications Manager-Use when the Cisco Unified Communications Manager sets the directory number type.  
  • Unknown-Use when the dialing plan is unknown.  
  • National-Use when you are dialing within the dialing plan for your country.  
  • International-Use when you are dialing outside the dialing plan for your country.  
  • Subscriber-Use when you are dialing a subscriber by using a shortened subscriber number. |
Choose the format for the numbering plan in calling party directory numbers. Cisco Unified Communications Manager sets the calling DN numbering plan. Cisco recommends that you do not change the default value unless you have advanced experience with dialing plans such as NANP or the European dialing plan. You may need to change the default in Europe because Cisco Unified Communications Manager does not recognize European national dialing patterns. You can also change this setting when you are connecting to PBXs by using routing as a non-national type number.

Choose one of the following options:

- **Cisco Unified Communications Manager** - Use when the Cisco Unified Communications Manager sets the Numbering Plan in the directory number.
- **ISDN** - Use when you are dialing outside the dialing plan for your country.
- **National Standard** - Use when you are dialing within the dialing plan for your country.
- **Private** - Use when you are dialing within a private network.
- **Unknown** - Use when the dialing plan is unknown.

### Called party number transformations settings

Called party transformations settings allow you to manipulate the dialed digits, or called party number, for outgoing calls. Examples of manipulating called numbers include appending or removing prefix digits (outgoing calls), appending area codes to calls dialed as seven-digit numbers, appending area codes and office codes to interoffice calls dialed as four- or five-digit extensions, and suppressing carrier access codes for equal access calls.

Configuration of called party transformations settings that are used in route lists occurs in the individual route groups that comprise the list. The called party transformations settings that are assigned to the route groups in a route list override any called party transformations settings that are assigned to a route pattern or translation pattern that is associated with that route list.

You can set the following called party transformation settings in the route group, route pattern, and translation pattern configuration:

- **Discard Digits**
- **Called Party Transform Mask**
- **Prefix Digits (Outgoing Calls)**
- **Called Party Number Type**
- **Called Party Numbering Plan**
The following table describes the fields, options, and values that are used to specify called party number transformations.

**Table 19: Called Party Number Transformations Settings**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Route Group Configuration</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Discard Digits</strong></td>
<td>This field contains a list of discard patterns that control the discard digit instructions. For example, in a system where users must dial 9 to make a call to the public switched telephone network (PSTN), the PreDot discard pattern causes the 9 to be stripped from the dialed digit string.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Any setting other than the default setting of &lt;None&gt; overrides the setting in the route pattern. The &lt;None&gt; setting means “do not discard digits.”</td>
</tr>
<tr>
<td><strong>Called Party Transform Mask</strong></td>
<td>This field specifies the called party transform mask for all calls that are routed through this route group. Valid values for this field range from 0 through 9, the wildcard character X, and characters *, +, and #. You can also leave this field blank. If this field is blank, no transformation takes place; Cisco Unified Communications Manager sends the dialed digits exactly as dialed. The called party transform mask can contain up to 50 digits.</td>
</tr>
<tr>
<td><strong>Prefix Digits (Outgoing Calls)</strong></td>
<td>This field contains a prefix digit or a set of Prefix Digits (Outgoing Calls) that are appended to the called party number on all calls that are routed through this route group. Valid values for this field range from 0 through 9, the characters *, +, and #, and blank. Prefix Digits (Outgoing Calls) can contain up to 50 digits on route patterns or up to 24 digits on DNs.</td>
</tr>
<tr>
<td>Field Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Called Party Number Type     | Choose the format for the number type in called party directory numbers. Cisco Unified Communications Manager sets the called directory number (DN) type. Cisco recommends that you do not change the default value unless you have advanced experience with dialing plans such as NANP or the European dialing plan. You may need to change the default in Europe because Cisco Unified Communications Manager does not recognize European national dialing patterns. You can also change this setting when you are connecting to a PBX that expects the called directory number to be encoded to a non-national type numbering plan. Choose one of the following options:  
  • Cisco Unified Communications Manager-Use when the Cisco Unified Communications Manager sets the directory number type.  
  • Unknown-Use when the dialing plan is unknown.  
  • National-Use when you are dialing within the dialing plan for your country.  
  • International-Use when you are dialing outside the dialing plan for your country.  
  • Subscriber-Use when you are dialing a subscriber by using a shortened subscriber number. |
| Called Party Numbering Plan  | Choose the format for the numbering plan in called party directory numbers. Cisco Unified Communications Manager sets the called DN numbering plan. Cisco recommends that you do not change the default value unless you have advanced experience with dialing plans such as NANP or the European dialing plan. You may need to change the default in Europe because Cisco Unified Communications Manager does not recognize European national dialing patterns. You can also change this setting when you are connecting to PBXs by using routing as a non national type number. Choose one of the following options:  
  • Cisco Unified Communications Manager-Use when the Cisco Unified Communications Manager sets the Numbering Plan in the directory number.  
  • ISDN-Use when you are dialing outside the dialing plan for your country.  
  • National Standard-Use when you are dialing within the dialing plan for your country.  
  • Private-Use when you are dialing within a private network.  
  • Unknown-Use when the dialing plan is unknown. |
Caller Identification and restriction

Cisco Unified Communications Manager provides the following types of caller identification information:

- Calling Line Identification (CLID)—Provides the called party with the extension or directory number of the calling party on a display.
- Calling Name Identification—Provides the called party with the name of the calling party on a display.
- Connected Line Identification—Provides the calling party with the phone number of the connected party on a display.
- Connected Name Identification—Provides the calling party with the name of the connected party on a display.

Cisco Unified Communications Manager provides flexible configuration options to allow and to restrict the display of the line and name information for both calling and connected parties.

Calling party presentation and restriction settings

Calling party presentation information controls whether to display the phone number and name information that Cisco Unified Communications Manager sends with setup messages for an outgoing call. Cisco Unified Communications Manager uses the following fields to provide these supplementary services:

- Calling Line ID Presentation field—Calling line identification presentation (CLIP) or calling line identification restriction (CLIR)
- Calling Name Presentation field—Calling name presentation (CNIP) or calling name restriction (CNIR)

You can use the Calling Party Presentation field in the Gateway Configuration window to control whether the CLID displays for all outgoing calls on the gateway. To control the CLID display on a call-by-call basis, you use the Calling line ID Presentation field in Route Pattern Configuration or Translation Pattern Configuration windows. You can also configure the Calling Line ID Presentation field in the Calling Party Transformation Pattern Configuration window.

Configure Calling Line ID Presentation and Connected Line ID Presentation, in combination with the Ignore Presentation Indicators (internal calls only) device-level parameter, to set up call display restrictions. Together, these settings allow you to selectively present or block calling and/or connected line display information for each call.
The following example describes how calling line ID presentation works. When a user makes a call, Cisco Unified Communications Manager checks whether the dialed number matches a translation pattern. Cisco Unified Communications Manager finds a match and sets the presentation indicator to the value in the translation pattern Calling Line ID Presentation field, which specifies “restricted” in this example. Next, Cisco Unified Communications Manager checks and finds a match on a route pattern that is configured for the dialed number. Cisco Unified Communications Manager checks the Calling Line ID Presentation field and finds that the value specifies “default.” The presentation indicator remains as “restricted” because the previous setting is unchanged when default is set.

The gateway Calling Party Presentation field gets checked last. In this example, the value specifies “allowed” and overrides the previous calling line ID presentation indicator to allow the calling party number to display on the called party phone. Therefore, the calling line ID presentation field indicator changed from “restricted” at the time that the calling party initiated the call to “allowed” by the time that Cisco Unified Communications Manager sends the call setup message to the endpoint device.

You can configure line and name presentation or restriction on a call-by-call basis for outgoing calls and incoming calls by using the Route Pattern Configuration or Translation Pattern Configuration windows.

For the gateway, you can only configure calling line ID presentation for outgoing calls. For incoming calls, Cisco Unified Communications Manager uses the Connected Line ID Presentation field for the gateway to specify whether to allow or restrict the connected party number to display on the calling party phone. Gateway settings only apply in these two situations, and these settings override all other settings. For the gateway, you can only configure calling and connected line presentation. No settings exist to control name presentation on the gateway.

The type of device control protocol that handles the call limits caller name and number information. See Table 14-12 for a list of protocols with the supported caller name and number information.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Calling Party Presentation (outgoing call)</td>
<td>This field determines whether the calling party phone number displays on the called party phone display screen. The Gateway Configuration, the Route Pattern Configuration, and the Translation Pattern Configuration windows use the Calling Line Presentation field. The following list gives the options for this field:</td>
</tr>
<tr>
<td></td>
<td>• Default: If default is set, calling line ID presentation does not get modified.</td>
</tr>
<tr>
<td></td>
<td>• Allowed: Use this setting to permit the calling party phone number to display in the called party phone display.</td>
</tr>
<tr>
<td></td>
<td>• Restricted: Use this setting to display “Private” in the called party phone display and block the display of the calling party phone number.</td>
</tr>
</tbody>
</table>

Note: To control the name display for non-QSIG trunks, you must enable the Display IE Delivery field or Send Calling Name in Facility IE field in the Gateway Configuration window.

Table 14-10 describes the fields, options, and values that are used to specify calling party presentations.

Table 20: Calling Party Presentation Settings
### Field Name | Description
--- | ---
Calling Name Presentation (outgoing call) | This field determines whether the name of the calling party displays on the called party phone display. The Route Pattern Configuration and Translation Pattern Configuration windows use the Calling Name Presentation field. The following list gives the options for this field:
- **Default**: If default is set, calling name presentation does not get modified.
- **Allowed**: Use this setting to display the calling party name in the called party phone display.
- **Restricted**: Use this setting in the route patterns or translation patterns configuration displays “Private” in the called party phone display.

**Note** | The gateway has no setting for calling name presentation.

Calling Line ID Presentation (incoming call) | If the incoming call goes through a translation pattern or route pattern and the calling line ID presentation setting is allowed or restricted, the calling line presentation gets modified with the translation or route pattern setting. If the call comes into the Cisco Unified Communications Manager system and then goes out to a PBX or the PSTN, the outgoing call rules apply.

**Note** | The Calling Party Presentation setting controls outgoing calls only.

Calling Name Presentation (incoming call) | If the incoming call goes through a translation pattern or route pattern and the calling name presentation setting is allowed or restricted, the calling name presentation gets modified with the translation or route pattern setting. If the call comes into the Cisco Unified Communications Manager system and then goes out to a PBX or the PSTN, the outgoing call rules apply.

**Note** | The gateway has no settings to control name information.

### Connected party presentation and restriction settings

Connected party presentation information controls whether to display the phone number and name information that Cisco Unified Communications Manager receives with an incoming call. Cisco Unified Communications Manager uses the following fields to provide these supplementary services:

- Connected Line ID Presentation field-Connected line identification presentation (COLP) or connected line identification restriction (COLR)
- Connected Name Presentation field-Connected name presentation (CONP) or calling name restriction (CONR)

Connected party settings allow you to display or restrict the display of the phone number and name of the connected party on the calling party phone. Translation Pattern Configuration and Route Pattern Configuration windows include these two settings. The calling party receives the connected name information after the call connects to Cisco Unified Communications Manager and the terminating phone.
The following example describes how connected line ID works. When Cisco Unified Communications Manager receives an incoming call, it checks whether a translation pattern is configured for the incoming number. Cisco Unified Communications Manager uses the value in the Connected Line ID Presentation field that specifies “restricted” for this example. Next, if a route pattern is configured for the incoming call, the value in the Connected Line ID Presentation field gets checked. In this example, the value specifies “default,” so the indicator remains as “restricted,” which prevents the connected party number from displaying on the calling party phone.

For incoming calls only, the gateway Connected Line ID Presentation field value gets checked last and is set for “allowed” in this example. The gateway setting specifies whether the connected party number can display on the calling party phone. In this case, Cisco Unified Communications Manager sends “allowed” in the CONNECT message, so the connected line can display on the originating caller phone display.

You can configure connected line and name presentation or restriction on a call-by-call basis for outgoing calls and incoming calls by using the Route Pattern Configuration or Translation Pattern Configuration windows.

For incoming calls on the gateway, you use the Connected Line ID Presentation field to specify whether to allow or restrict the display of the connected party number on the calling party phone. Gateway settings only apply to line presentation settings and override all other settings.

---

**Note**

For the gateway, you can only configure calling and connected line presentation options. No settings exist for name presentation on the gateway.

When a call routes through a translation or route pattern and connected line presentation is allowed, the phone updates the connected number presentation for the modified number, unless the Always Display Original Dialed Number service parameter is set to true. When this setting is true, the originating phone displays only the dialed digits for the duration of the call. Only phones that are running SCCP support this option.

This table describes the fields, options, and values that are used to specify connected party presentations.

### Table 21: Connected Party Presentation Settings

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connected Line ID Presentation (outgoing call)</td>
<td>In the Route Pattern Configuration and the Translation Pattern Configuration windows, this field determines whether the connected party number displays on the calling party phone display.</td>
</tr>
</tbody>
</table>

The following list gives the options for this field:

- **Default**: If default is set, connected line ID presentation does not get modified.
- **Allowed**: Use this setting to display the connected line number that Cisco Unified Communications Manager received in protocol messages on the calling party phone display.
- **Restricted**: Use this setting to block the connected party number from displaying in the calling party phone display, and “Unknown Number” displays instead.

**Note** This setting applies to internal calls and calls on QSIG connections only.
**Field Name** | **Description**
---|---
Connected Name Presentation (CONP/CONR) (outgoing call) | This field determines whether the connected party name displays on the calling party phone display. The Route Pattern Configuration and Translation Pattern Configuration windows use the Connected Name Presentation field. The following list gives the options for this field:
- Default: If default is set, calling name presentation does not get modified.
- Allowed: Use this setting to display the connected party name that Cisco Unified Communications Manager received in protocol messages in the calling party phone display.
- Restricted: Use this setting to block the connected party name from displaying, and display “Unknown” in the calling party phone display.

Connected Line ID Presentation (incoming call) | If the incoming call goes through a translation or route pattern and the connected line ID presentation field is set to allowed or restricted, the connected line presentation indicator gets modified with the translation or route pattern setting.

**Note** | The Connected Line ID Presentation setting on the gateway determines if the connected party number can display on the originating party phone. If the call comes into the Cisco Unified Communications Manager system and then goes out to a PBX or the PSTN, the outgoing call rules apply.

Connected Name Presentation (incoming call) | If the incoming call goes through a translation or route pattern and the connected name presentation setting is set to allowed or restricted, the connected name presentation gets modified with the translation or route pattern setting. If the call comes into the Cisco Unified Communications Manager system and then goes out to a PBX or the PSTN, the outgoing call rules apply.

**Note** | The gateway has no settings to control name information.

---

**Caller Identification support with device control protocols in Cisco Unified Communications Manager**

Cisco Unified Communications Manager provides support for caller name and number identification presentation based on the device control protocols that handle the call. Not all device protocols provide caller number and name information in the protocol messages.

Table 14-12 summarizes which protocols support caller identification services.

**Table 22: Caller Identification Information Supported by Device Control Protocols**

<table>
<thead>
<tr>
<th>Device Control Protocol</th>
<th>Calling Line</th>
<th>Calling Name</th>
<th>Connected Line</th>
<th>Connected Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Phones with SCCP</td>
<td>provides line number</td>
<td>provides name associated with DN</td>
<td>displays number when received</td>
<td>displays name when received</td>
</tr>
</tbody>
</table>
### Device Control Protocol | Calling Line | Calling Name | Connected Line | Connected Name
--- | --- | --- | --- | ---
MGCP Stations (FXS) | provides line number | provides name associated with DN | not supported | displays name when received
MGCP Trunk (FXO, T1CAS) | supported on FXO incoming ports only | supported on FXO incoming ports only | supported on FXO incoming ports only | supported on FXO incoming ports only
H.323 Trunk | calling line sent in H.225 SETUP | supported by using DISPLAY IE in H.225 messages for intercluster trunks only | supported by H.225 NOTIFY for intercluster trunks only | supported by DISPLAY IE in H.225 messages for intercluster trunks only
PRI Trunk | calling line in PRI SETUP | supported by using FACILITY IE in PRI messages | not supported | supported by using FACILITY IE in PRI messages
QSIG Trunk | calling line in QSIG SETUP | supported by using FACILITY IE in QSIG messages | supported by QSIG CONNECT | supported by using FACILITY IE in QSIG messages
SIP Trunk | calling line included in From and Remote-Party-ID headers | calling name included in From and Remote-Party-ID headers | connected line included in Remote-Party-ID header | connected name included in Remote-Party-ID header

**Related Topics**
- Special characters and settings, on page 161
- Calling and Called party transformations, on page 177
- Enhanced Call Identification services, on page 413

**Route plan report**

The route plan report comprises a listing of all unassigned directory numbers (DN), call park numbers, call pickup numbers, conference numbers (Meet-Me numbers), directory numbers, route patterns, translation patterns, voice-mail ports, and message-waiting indicators.

The route plan report allows you to view either a partial or full list and to go directly to the associated configuration windows by choosing a route pattern, partition, route group, route list, directory number, call park number, call pickup number, conference number (Meet-Me number), or gateway.

Using the route plan report, you can get a list of unassigned directory numbers and delete those numbers from the Cisco Unified Communications Manager database, if required.

In addition, the route plan report allows you to save report data into a .csv file that you can import into other applications such as the Bulk Administration Tool (BAT). The .csv file contains more detailed information, including directory numbers (DN) for phones, route patterns, and translation patterns. See the Cisco Unified Communications Manager Administration Guide for more information.
See the Local route groups and called party transformations, on page 151 for details of route plan reports in a local route group scenario.
Directory numbers

This chapter provides information about using the Directory Number Configuration window in Cisco Unified Communications Manager Administration, to configure and modify directory numbers (lines) that are assigned to phones. Keep in mind, however, that directory numbers (DNs) do not always associate with devices.

- Configure directory number, page 191
- Characteristics of directory numbers, page 192
- Shared line appearance, page 193
- Manage directory numbers, page 197
- Directory number features, page 198
- Make and receive multiple calls per directory number, page 199
- Search by directory number, page 201
- Dependency records, page 202

Configure directory number

Using the Directory Number Configuration window in Cisco Unified Communications Manager Administration, you can configure and modify directory numbers (lines) that are assigned to phones. Keep in mind, however, that directory numbers (DNs) do not always associate with devices.

Tip
If you are using autoregistration, Cisco Unified Communications Manager adds the phone and automatically assigns the directory number.

Note
For information on how to configure Private Line Automatic Ringdown (PLAR), see Manage directory numbers, on page 197.

The steps to manually configure a directory number in Cisco Unified Communications Manager Administration are as follows. For more information on directory numbers, see the Characteristics of directory numbers, on page 192.
Procedure

Step 1  If you want to configure a DN for a phone, add and configure the phone. You may need the following information about the phone:

• Model
• MAC address
• Physical location of the phone
• Cisco Unified Communications Manager user to associate with the phone
• Partition, calling search space, and location information, if used
• Number of lines and associated DNs to assign to the phone

Step 2  Add and configure lines (DNs). Configure DNs either from the Directory Number Configuration window or, if you want to configure a DN for a phone, from the Phone Configuration window. You can also configure phone features such as call park, call forward, and call pickup.

Step 3  Configure speed-dial buttons. You can configure speed-dial buttons for phones if you want to provide speed-dial buttons for users or if you are configuring phones that do not have a specific user who is assigned to them. Users can change the speed-dial settings on their phones by using Cisco Unified CM User Options.

Step 4  Configure Cisco Unified IP Phone services. You can configure services for Cisco Unified IP Phones 7970, 7960, 7940, 7912, and 7905 and Cisco IP Communicator if you want to provide services for users or if you are configuring phones that do not have a specific user who is assigned to them. Users can change the services on their phones by using the Cisco Unified CM User Options.

Step 5  Customize phone button templates and softkey templates, if required. Configure templates for each phone.

Step 6  Assign services to phone buttons, if required.

Step 7  Provide power, install, verify network connectivity, and configure network settings for the Cisco Unified IP Phone.

Step 8  Associate a user with the phone (if required).

Characteristics of directory numbers

You can configure up to 200 calls for a line on a device. As you configure the number of calls for one line, the calls that are available for another line decrease. Cisco Unified IP Phones that support the multicall display (such as a Cisco Unified IP Phone 7960) support up to 200 calls per DN and 2 calls per DN for non-multicall display devices (such as Cisco Unified IP Phone 7905).

The Cisco Unified IP Phone displays the following information about each line:

• Unique call identifier (from 1 to 200). This identifier remains consistent across all multicall display devices that have a shared-line appearance.

• Call select status, an icon that shows the state of the currently selected call

• Call information such as calling party or called party

• Call state icon such as connected or hold
• Duration of a call

**User/Phone Add and Directory Numbers**

The End User, Phone, DN, and LA Configuration window allows all-at-once addition of a new end user and a new phone that is associated with the new end user. You can associate a directory number (existing or new) and line appearance for the new end user by using the same window. To access the End User, Phone, DN, and LA Configuration window, choose the **User Management > User/Phone Add** menu option.

---

**Note**

The End User, Phone, DN, and LA Configuration window only allows addition of a new end user and a new phone. The window does not allow entry of existing end users or existing phones.

---

### Shared line appearance

You can set up one or more lines with a shared-line appearance. A Cisco Unified Communications Manager system considers a directory number to be a shared line if it appears on more than one device in the same partition. For example, if directory number 9600 on phone A is in the partition called Dallas and on phone B in the partition called Texas, that directory number does not represent a shared-line appearance. (Ensure the directory number 9600 for phone A and phone B are in the same partition; for example, Dallas.)

In a shared-line appearance, for example, you can set up a shared line, so a directory number appears on line 1 of a manager phone and also on line 2 of an assistant phone. Another example of a shared line involves a single incoming 800 number that is set up to appear as line 2 on every sales representative phone in an office. You can also choose to update a directory number and have the updates apply to all devices that share the directory number.

The following information provides tips about and lists the restrictions for using shared-line appearances with Cisco Unified Communications Manager.

**Shared Line Tips**

Use the following tips when configuring shared lines:

- You create a shared-line appearance by assigning the same directory number and route partition to different devices.

- If multiple devices share a line, each device name displays in the Associated Devices pane of the directory number in the Directory Number Configuration window in Cisco Unified Communications Manager Administration.

- If you change the Calling Search Space or Call Forward and Pickup settings on any device that uses the shared line, the changes apply to all devices that use that shared line.

---

**Note**

Shared lines always have identical DN settings, except for the field sections in the Directory Number Configuration window that contain the naming convention “on Device SEPXXXXXXXXXXXXX,” which are maintained/mapped to a specific device.
• To stop sharing a line appearance on a device, change the directory number or partition name for the line and update the directory number in the Directory Number Configuration window in Cisco Unified Communications Manager Administration.

• In the case of a shared-line appearance, Remove From Device removes the directory number on the current device only and does not affect other devices.

• Most devices with a shared-line appearance can make or receive new calls or resume held calls at the same time. Incoming calls display on all devices that share a line, and anyone can answer the call. Only one call remains active at a time on a device.

Note: Cisco Unified IP Phones 7905, 7912, 7940, and 7960 that are running SIP will not display remote-in-use calls and cannot do remote resume (cannot pick up a held line that is shared). These phones that are running SIP do not support shared-line features such as Single Button Barge/cBarge, Barge, cBarge, and Privacy.

• Call information (such as calling party or called party) displays on all devices that are sharing a line. If one of the devices turns on the Privacy feature, other devices that share the line will not see outbound calls that are made from the device that turned on privacy. All devices will still see inbound calls to the shared line.

• Devices with shared-line appearances can initiate independent transfer transactions.

• Devices with shared-line appearances can initiate independent conference transactions.

• Devices with shared-line appearance support the Call Forward Busy Trigger and the Maximum Number of Calls settings. You can configure Call Forward Busy Trigger per line appearance, but the configuration cannot exceed the maximum number call setting for that directory number.

The following example demonstrates how three Cisco Unified IP Phones with the same shared-line appearance, directory number 2000, use Call Forward Busy Trigger and Maximum Number of Calls settings. This example assumes that two calls occur. The following values configuration applies for the devices:

• Cisco Unified IP Phone 1—Configured for a maximum call value of 1 and busy trigger value of 1
• Cisco Unified IP Phone 2—Configured for a maximum call value of 1 and busy trigger value of 1
• Cisco Unified IP Phone 3—Configured for a maximum call value of 2 and busy trigger value of 2

When Cisco Unified IP Phone User 1 dials directory number 2000 for the first call, all three devices ring. The user for Cisco Unified IP Phone 3 picks up the call, and Cisco Unified IP Phones 1 and 2 go to remote in use. When the user for Cisco Unified IP Phone 3 puts the call on hold, user can retrieve the call from Cisco Unified IP Phone 1 or Cisco Unified IP Phone 2. When User 2 dials directory number 2000 for the second call, only Cisco Unified IP Phone 3 rings.

The following example demonstrates how an H.323 client, MGCP POTS phone, and Cisco Unified IP Phone with the same shared line appearance, directory number 2000, can use the Call Forward Busy Trigger and the Maximum Number of Calls settings. This example assumes that two calls occur. The following values configuration applies for the devices:

• H.323 client—Configured for a maximum call value of 1 and busy trigger value of 1
• MGCP POTS Phone—Configured for a maximum call value of 1 and busy trigger value of 1
• Cisco Unified IP Phone—Configured for a maximum call value of 2 and busy trigger value of 2
When User 1 dials directory number 2000 for the first call, all three devices ring. The user for the Cisco Unified IP Phone picks up the call; when the user for Cisco Unified IP Phone puts the call on hold, the user(s) for H323 client and MGCP POTS phone cannot retrieve the call. If User 2 dials directory number 2000 for the second call, all three devices (IP phone, MGCP POTS phone, H.323 client) ring, and all three users can answer the call.

The Update Directory Number of All Devices Sharing this Line checkbox, in the Directory Number Configuration window, determines whether a shared directory number gets updated to all devices that share the number. See the Manage directory numbers, on page 197 for more information.

A shared-line phone should not be able to interact with the call that it rejects, due to the limitation of the maximum number of calls per DN or for other reasons. For example, A and A1 share the same DN. A1 and A have the maximum number of calls set to 1 and 2, respectively. When C and D call the share line DN, A1 answers these two calls. A can only interact with the first call, as it rejects the second call due to its own maximum number of calls per DN limitation. For this reason, Cisco recommends that the same value be configured for the maximum number of calls for all shared-line MCID devices. For N number of devices that share the same line, ensure both Maximum Calls setting and Busy Trigger setting are set to N. This allows each shared-line user to receive at least one call.

The shared-line phone should not interact with the call that it does not receive (because the Line Control does not maintain call information). So, a newly registered device will not recognize any existing calls on that line. The newly registered device cannot resume any held call if the call started before this device was registered with the Line Control. For example, A and A1 share the same line, A is powered down (or logged out for the extension mobility user), and A1 receives an active call. After phone A is on and it registers with Cisco Unified Communications Manager, A should not see the existing active call in this line.

If shared-line phone calls should interact with each other, Cisco recommends that you set the maximum number of calls for all shared-lines MCID devices to 2*N, where N specifies the number of shared-line devices.

- A phone user can view held calls on shared-line appearances on the phone. For example, a phone user can determine whether the call was put on hold by the phone user locally at the primary device or by another party remotely on a shared device. You do not need to perform any configuration for this feature to work. For more information on viewing held calls for shared lines, see the Cisco Unified IP Phone documentation that supports your phone model.

- If you want to do so, you can check the Log Missed Calls checkbox in Cisco Unified Communications Manager Administration, so Cisco Unified Communications Manager logs missed calls in the call history for a specified shared line appearance on a phone.

This feature works if a phone user logs in to a phone via Cisco Extension Mobility.

The examples in Table 15-2, which use the following phones, describe how the missed call logging feature works for shared lines:

- Phone A, which has directory number 1000 that is configured for the first line and directory number 2000 for the second line, which is shared with phone B.

- Phone B, which has directory number 2000 that is configured as the first line, which is shared with phone A, and directory number 3000 that is configured as the second line.

- Phone C, which places the calls.
Table 23: Examples of How Logging Works for Missed Calls With Shared Lines

<table>
<thead>
<tr>
<th>Phone A</th>
<th>Phone B</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Phone C calls directory number (DN) 1000.</td>
<td>Not applicable</td>
</tr>
<tr>
<td>• The Logged Missed Calls check box displays</td>
<td></td>
</tr>
<tr>
<td>as checked for DN 1000.</td>
<td></td>
</tr>
<tr>
<td>• Missed calls get logged to DN 1000.</td>
<td></td>
</tr>
<tr>
<td>If the Logged Missed Calls check box displays</td>
<td></td>
</tr>
<tr>
<td>as unchecked, missed calls do not get</td>
<td></td>
</tr>
<tr>
<td>logged to DN 1000.</td>
<td></td>
</tr>
<tr>
<td>• Phone C calls directory number (DN) 2000.</td>
<td>• Phone C calls DN 2000, which is a shared</td>
</tr>
<tr>
<td>• The Logged Missed Calls check box displays</td>
<td>line appearance.</td>
</tr>
<tr>
<td>as checked for DN 2000.</td>
<td>• Logging displays for the shared line</td>
</tr>
<tr>
<td>• Missed calls get logged to DN 2000.</td>
<td>appearance on Phone B because the Logged</td>
</tr>
<tr>
<td>If the Logged Missed Calls check box displays</td>
<td>Missed Calls check box is checked for DN</td>
</tr>
<tr>
<td>as unchecked, missed calls do not get</td>
<td>2000.</td>
</tr>
<tr>
<td>logged to DN 2000.</td>
<td></td>
</tr>
</tbody>
</table>

Shared Line Restrictions

The following restrictions apply to shared lines:

• Do not use shared-line appearances on any Cisco Unified IP Phone that requires autoanswer capability and do not turn on auto answer for a shared-line appearance.

• Do not configure shared-line appearances on the primary lines of the phones; for example, if two phones have a shared-line appearance, only one of the phones should have the primary line configured as shared (the other phone should have the secondary line configured as shared).

• Barge, cBarge, and Privacy work with shared lines only.

• Cisco recommends that you do not configure shared lines for Cisco Unified IP Phones, H.323 clients, and MGCP POTS phones; likewise, Cisco recommends that you do not configure shared lines for H.323 clients and MGCP POTS phones. If you configure the same shared-line appearance for a H.323 client, a MGCP POTS phone, for example, NetMeeting, and a Cisco Unified IP Phone, you cannot use the hold/resume feature on the H.323 client or MGCP POTS phone.

• Cisco recommends that you do not configure shared lines for Cisco Unified IP Phones 7905, 7912, 7940, and 7960 that are running SIP because these phones cannot pick up held calls on shared lines nor can they use the shared-line features Single Button Barge/cBarge, Barge, cBarge, and Privacy.

• Cisco Unified IP Phones 7906, 7911, 7941, 7961, 7970, and 7971 that are running SIP have the capability of supporting multiple lines with the same directory number in different partitions. However, configuring and using other phones that are running SIP with multiple lines with the same directory number is not supported.
• If the number of shared-line users in the conference is equal to or greater than the configuration for the Maximum Number of Calls setting for the device from which you are attempting to barge, the phone displays the message, Error Past Limit.

Manage directory numbers

Directory numbers associate with devices such as phones, route points, CTI ports, and H.323 clients. Administrators manage directory numbers from the Directory Number Configuration and Route Plan Report windows in Cisco Unified Communications Manager Administration. Use the Directory Number Configuration window or the Phone Configuration window to add, update, and remove directory numbers from a device, route point, or port. Use the Route Plan Report window to delete or update unassigned directory numbers from Cisco Unified Communications Manager database.

Note

Do not associate a directory number with a CTI route point or CTI port if the directory number is a member of a line group.

The Directory Number Configuration window contains two check boxes: Active and Update Directory Number of All Device Sharing this Line.

Active Check Box

The Active check box, which only displays for unassigned directory numbers, determines whether the directory number gets loaded and used by Cisco Unified Communications Manager. By checking the check box, the directory number gets loaded and used by Cisco Unified Communications Manager. For example, the directory number belonged to an employee who left the company. The directory number had certain settings that were configured, such as call forwarding to voice-messaging system. By leaving the directory number active, a call that is intended for the directory number will get forwarded. This eliminates the need to reconfigure another employee to have the same call-forwarding options. If the check box is not checked, the directory number will not get loaded by Cisco Unified Communications Manager, which results in settings that are configured for that DN to not be used (for example, call forward destinations), and callers will not get their call forwarded properly.

Update Directory Number of All Devices That Share This Line Check Box

This check box determines whether a shared directory number gets updated to all devices that share the number. When the check box is checked, all devices that share the directory number will receive the directory number change. If the check box remains unchecked, only the current device that displays in the window gets the directory number changed, and all other devices that share the directory number remain unchanged.

Note

This check box only applies to the actual directory number and partition. It does not apply to the other device settings such as voice-messaging profile, call-forwarding options, or MLPP. If any of these settings are changed for a shared line, all devices get changed.
Directory number features

Cisco Unified Communications Manager enables you to configure the following features for directory numbers: call waiting and call forward.

For information about features that relate to phones, see the Phone features, on page 520. The following features get configured for phones: barge, privacy release, call back, call park, call pickup, immediate divert, malicious call identification, quality report tool, service URL, and speed dial and abbreviated dial.

Call Forward

Call forward allows a user to configure a Cisco Unified IP Phone, so all calls that are destined for it ring another phone. The following types of call forward exist:

- Call forward all: Forwards all calls.
- Call forward busy: Forwards calls only when the line is in use and busy trigger setting is reached.
- Call forward no answer: Forwards calls when the phone is not answered after the configured no answer ring duration, or if the destination is unregistered.
- Call forward no coverage: Forwards calls when call either exhausts or times out, and the associated hunt-pilot for coverage specifies Use Personal Preferences for its final forwarding.

You can configure each call forward type for internal and external calls that can be forwarded to voice-messaging system, dialed destination number, or calling search space.

Cisco Unified Communications Manager supports a secondary Calling Search Space (CSS) for Call Forward All (CFA) field. The secondary CSS for CFA combines with the existing CSS for CFA to allow the support of the alternate CSS system configuration. When CFA is activated, only the primary and secondary CSS for CFA get used to validate the CFA destination and redirect the call to the CFA destination. If these fields are empty, the null CSS gets used. The combination of the line CSS and device CSS no longer gets used when the CSS for CFA is None. Only the CSS fields that are configured in the primary CSS for CFA and secondary CSS for CFA fields get used. If CFA is activated from the phone, the CFA destination gets validated by using the CSS for CFA and the secondary CSS for CFA, and the CFA destination gets written to the database. When the CFA is activated, the CFA destination always gets validated against the CSS for CFA and the secondary CSS for CFA.

The administrator can configure call-forward information display options to the original dialed number or the redirected dialed number or both. The administrator can enable or disable the calling line ID (CLID) and calling name ID (CNID). The display option gets configured for each line appearance.

The call forward busy trigger gets configured for each line appearance and cannot exceed the maximum number of calls that are configured for a line appearance. The call forward busy trigger determines how many active calls exist on a line before the call forward busy setting gets activated (for example, 10 calls).

The call forward no answer ring duration gets configured for each line appearance, and the default specifies 12 seconds. The call forward no answer ring duration determines how long a phone rings before the call forward no answer setting gets activated.

Tip

Keep the busy trigger slightly lower than the maximum number of calls, so users can make outgoing calls and perform transfers.
Configure call forward in the Directory Number Configuration window in Cisco Unified Communications Manager Administration.

Cisco Unified Communications Manager provides a service parameter (CFA Destination Override) that allows the administrator to override Call Forward All (CFA) when the target of the CFA calls the initiator of the CFA, so the CFA target can reach the initiator for important calls. In other words, when the user to whom calls are being forwarded (the target) calls the user whose calls are being forwarded (the initiator), the phone of the initiator rings instead of call forwarding back to the target. The override works whether the CFA target phone number is internal or external.

When the CFA Destination Override service parameter is set to False (the default value), no override occurs. Ensure the service parameter is set to True for CFA override to work.

---

**Note**

CFA override only takes place if the CFA destination matches the calling party and the CFA Destination Override service parameter is set to True. If the service parameter is set to True and the calling party does not match the CFA destination, CFA override does not take place, and the CFA remains in effect.

---

**Call Waiting**

Call waiting lets users receive a second incoming call on the same line without disconnecting the first call. When the second call arrives, the user receives a brief call-waiting indicator tone, which is configured with the Ring Setting (Phone Active) in the Directory Number Configuration window.

Configure call waiting in the Directory Number Configuration window in Cisco Unified Communications Manager Administration by setting the busy trigger (greater than 2) and maximum number of calls.

---

**Tip**

To configure call waiting for phones with no display (such as the Cisco IP Phone 30 VIP), set the busy trigger to 2 and the maximum number of calls to 2.

---

**Note**

The user can invoke the Cancel Call Waiting feature, which enables the user to block the operation of call waiting for one call. During this call, the Call Waiting service is rendered inactive, so that anyone calling the user receives the normal busy treatment, and no call waiting tones interrupt the call. For more information on the cancel call waiting feature, see the Cancel Call Waiting, on page 524.

---

**Make and receive multiple calls per directory number**

Cisco Unified Communications Manager supports various behaviors when users make and receive multiple calls per DN: Transfer/Direct Transfer and Conference/Join.

Transfer allows different line appearances in one device to initiate independent transfer transactions and allows multiple transfer transactions per line appearance per device.

Conference allows different line appearances in one device to initiate independent conference transactions and allows multiple conference transactions per line appearance per device.
Devices that do not support multicalled display, such as Cisco Unified IP Phone 7910, cannot transfer or conference two existing calls together.

**Transfer and conference behavior**

If only one active call exists on the directory number, the first invocation of a feature results in putting the active call on hold and initiating a new call by using the same directory number. When the new call gets set up, the second invocation of the same feature starts the feature operation. The first invocation of Transfer/Conference will always initiate a new call by using the same directory number, after putting the active call on hold.

**Direct transfer and join behavior**

The following information describes Direct Transfer and Join behavior:

- Direct Transfer joins two established calls (call is in hold or in connected state) into one call and drops the feature initiator from the call. Direct Transfer does not initiate a consultation call and does not put the active call on hold.

- Join does not create a consultation call and does not put the active call on hold. To implement Join, choose at least two calls and then press the Join softkey on one of the calls. Join can include more than two calls, which results in a call with three or more parties. Join supports up to 16 participants in a call. To choose an active or held call, highlight the call and press the Select softkey. A checked indicator displays next to a selected call on the phone.

  The call that initiates the Join automatically gets included, even if it is not selected. The active call gets included even if not selected. If all the calls in the join represent a basic call, the call that initiated the join represents the primary call. If any call in the join is a conference call (that is, it was in a conference before being joined), that call represents the primary call.

  The selected status of the final call after the join depends on the selected status of the primary call before the join. If the primary call was selected, the final call remains selected after the join. This means that if that call is put on hold, shared lines would not be able to retrieve the call because the call is still selected. If the primary call was not selected, the final call remains unselected after the call.

- With the party entrance tone feature, a tone plays on the phone when a basic call changes to a multiparty call; that is, when a basic call changes to a barged call, cBarged call, ad hoc conference, meet-me conference, or a joined call. In addition, a different tone plays when a party leaves the multiparty call.

  When a joined call begins, Cisco Unified Communications Manager uses the party entrance tone configuration from the conference controller. Cisco Unified Communications Manager uses this configuration until the conference ends.

  To use the party entrance feature, ensure that you turned the privacy feature off for the devices and ensure that the controlling device for the multiparty call has a built-in bridge. In addition, either configure the Party Entrance Tone service parameter, which supports the Cisco CallManager service, or configure the Party Entrance Tone setting per directory number in the Directory Number Configuration window (Call Routing > Directory Number).
If more than one call in the join is a conference call, conference chaining occurs.

Note

Be aware that Private and Hidden calls are not recognized for Join.

Join Across Lines Behavior

The Join Across Lines feature allows a user to join calls that are on multiple lines—either on different directory numbers, or on the same directory number but on different partitions. To implement Join by using the Join Across Lines feature, press the Join softkey from an active call; then, press the line button for the call(s) that you want to include in the conference. If more than one call exists on the selected line, a window opens on the phone screen to prompt the user to select the call(s) to be joined. Select the call(s) and press Join to complete the action.

The call that initiates the Join automatically gets included, even if it is not selected. The active call gets included even if not selected. If all the calls in the join represent a basic call, the call that initiated the join represents the primary call. If any call in the join is a conference call (that is, it was in a conference before being joined), that call represents the primary call.

The selected status of the final call after the join depends on the selected status of the primary call before the join. If the primary call was selected, the final call remains selected after the join. This means that if that call is put on hold, shared lines cannot retrieve the call because the call is still selected. If the primary call was not selected, the final call remains unselected after the call.

Search by directory number

The following sections describe how to modify your search to locate a directory number. If you have thousands of directory numbers in your network, you may need to limit your search to find the directory number that you want. If you cannot locate a directory number, you may need to expand your search to include more directory numbers.

Note

Be aware that the directory number search is not case sensitive.

Searching by Directory Number

To search for a phone by its directory number (DN), choose Directory Number and either enter a search criteria (such as begins with or ends with) or click the Find button.

Note

Some directory numbers do not associate with phones. To search for those directory numbers, which are called unassigned DN, use the Route Plan Report window.
Searching by Route Partition

To search for a phone by its route partition, choose Route Partition and either enter a search criteria (such as begins with or ends with) or click the Find button.

Searching by Description

To search for a phone by its description, choose Description and either enter a search criteria (such as begins with or ends with) or click the Find button.

Search Within Results

To refine your search results, you can search for additional information. For example, if you search for directory numbers by directory number, you may want to search within the directory number results for DNs that share the same route partition. After you perform an initial search, check the Search Results check box. You can enter additional, or different, search criteria in the drop-down list boxes. Click Find again to search within the previous results.

Finding All Directory Numbers in the Database

To find all directory numbers that are registered in the database, choose Directory Number from the list of fields; choose “is not empty” from the list of patterns; then, click the Find button.

Dependency records

If you need to find the directory numbers that a specific phone is using or the phones to which a directory number is assigned, choose Dependency Records from the Related Links drop-down list box on the Cisco Unified Communications Manager Administration Phone Configuration or Directory Number Configuration window. The Dependency Records Summary window displays information about directory numbers that are using the phone. To find more information about the directory number, click the directory number, and the Dependency Records Details window displays. If the dependency records are not enabled for the system, the dependency records summary window displays a message.
Dial rules overview

This chapter provides information about dial rules. Cisco Unified Communications Manager supports different types of dial rules: Application Dial Rules, Directory Lookup Dial Rules, and SIP Dial Rules.

The administrator uses Application Dial Rules to add and sort the priority of dialing rules for applications such as Cisco Web Dialer and Cisco Unified Communications Manager Assistant. Application Dial Rules automatically strip numbers from or add numbers to telephone numbers that the user dials. For example, the dial rules automatically add the digit 9 in front of a 7-digit telephone number to provide access to an outside line.

In Cisco Unified Communications Manager Assistant, the assistant can perform a directory search from the assistant console. The assistant can drag and drop the directory entry to the My Calls panel on the assistant console, which invokes a call to the number that is listed in the entry. The dial rules apply to the number that is listed in the entry before the call gets made.

Cisco Unified Communications Manager performs system digit analysis and routing; however, the Cisco Unified IP Phone needs to know when enough digits are collected before call processing takes place, so the administrator configures SIP Dial Rules and adds the SIP dial rule to the phone.

- Application dial rules configuration design, page 203
- Application dial rules configuration error checking, page 204
- Directory lookup dial rules, page 205
- SIP dial rules, page 206

Application dial rules configuration design

The Application Dial Rule Configuration window includes the following information:

- Name-This field comprises a unique name for the dial rule that can contain up to 20 alphanumeric characters and any combination of spaces, periods (.), hyphens (-), and underscore characters (_).

- Description-This field comprises a brief description that you enter for the dial rule.

- Number Begins With-This field comprises the initial digits of the directory numbers to which you want to apply this application dial rule.

- Number of Digits-This required field comprises the initial digits of the directory numbers to which you want to apply this application dial rule.
• Total Digits to be Removed—This required field comprises the number of digits that you want Cisco Unified Communications Manager to remove from directory numbers that apply to this dial rule.

• Prefix With Pattern—This required field comprises the pattern to prepend to directory numbers that apply to this application dial rule.

• Application Dial Rule Priority—This field displays when you enter the Prefix With Pattern information. The field allows you to set the priority order of the application dial rules.

The following example provides a dial rule condition and the consequence when a dial rule is created.

**Condition**

• If the phone number begins with (the field is blank)—This condition leaves blank one or more digits at the beginning of the number that the user dialed. For example, if the user dialed 1, 1500, or 1500555, each would match the dial number 15005556262.

• and the number of digits is (the field is blank)—This condition leaves blank the total number of digits in the telephone number that the user dialed. For example, if the dial number is 915005556262, the number of digits equals 12.

**Consequence**

• Remove blank digits from the beginning—The application deletes this number of digits from the front of the dialed number. For example, if 4 is specified, and the dialed number is 15005556262, the application removes 1500, leaving 5556262.

• and prefix it with (this field is blank)—After removing the specified number of digits, the application adds this string of numbers to the front of the dialed number. For example, if 9 was specified, the application adds 9 to the front of the dialed number (could be specifying an outside line).

**Application dial rules configuration error checking**

The application dial rules perform the following error checking in the Dial Rule Creation section of the Dial Rules Configuration window:

• The phone number begins with field supports only digits and the characters +*#. The length cannot exceed 100 characters.

• The Number of Digits field supports digits between 1 and 100, as well as the plus sign (+), the asterisk (*), and the number sign (#). Enter the number of digits of the dialed numbers to which you want to apply this application dial rule. You cannot allow this field to be blank for a dial rule.

• The remove digits field supports only digits, and the value in this field cannot be more than the value in the number of digits is field.

• The prefix it with field supports only digits and the characters +*#. The length cannot exceed 100 characters.

• Ensure that dial rules are unique.

• You cannot allow the remove digits field and the prefix it with field both to be blank for a dial rule.
Directory lookup dial rules

The Directory Lookup Dial Rule Configuration window allows you to enter the following information for each dial rule:

• Name - This field comprises a unique name for the dial rule that can contain up to 20 alphanumeric characters and any combination of spaces, periods (.), hyphens (-), and underscore characters (_).

• Description - This field comprises a brief description that you enter for the dial rule.

• Number Begins With - This field comprises the initial digits of the directory numbers to which you want to apply this application dial rule.

• Number of Digits - This required field comprises the length of the directory numbers to which you want to apply this directory lookup dial rule.

• Total Digits to be Removed - This required field comprises the number of digits that you want Cisco Unified Communications Manager to remove from directory numbers that apply to this dial rule.

• Prefix With Pattern - This required field comprises the pattern to prepend to directory numbers that apply to this dial rule.

Directory Lookup Dial Rule Example

You can create a directory lookup rule that automatically adds 40852 to 5-digit numbers beginning with 5. Using this rule, the number 56666 becomes 4085256666. If 4085256666 matches a user in the directory, Cisco Unified Communications Manager displays the name in the Call Details window.

To create this rule, enter the following information on the Directory Lookup Dial Rules window:

• In the Number Begins With field, enter “5,” so the dial rule applies to numbers that begin with the number 5.

• In the Number of Digits field, enter the number of digits “5,” so the dial rule applies to numbers that contain 5 digits.

• In the Prefix With Pattern field, enter “40852,” so the dial rules prepends 40852 to numbers that apply to this dial rule.

Limitations

When creating a directory lookup rule, consider the following limitations:

• The phone number begins with field supports only digits and the characters +*#. The length cannot exceed 100 characters.

• The number of digits is field supports only digits, and the value in this field cannot be less than the length of the pattern that is specified in the pattern field.

• The remove digits field supports only digits, and the value in this field cannot be more than the value in the number of digits is field.

• The prefix it with field supports only digits and the characters +*#. The length cannot exceed 100 characters.

• You cannot allow both the remove digits field and the prefix it with field to be blank for a dial rule.
SIP dial rules

The administrator uses SIP dial rule configuration to configure dial plans for phones that are running SIP and associate them with the following phones that are running SIP:

- Cisco Unified IP Phones 7911, 7941, 7961, 7970, and 7971 that are running SIP. These phones use the 7940_7960_OTHER dial rules patterns. Key Press Markup Language (KPML) allows for the digits to be sent to Cisco Unified Communications Manager digit by digit; SIP Dial Rules allow for a pattern of digits to be collected locally on the phone prior to sending to Cisco Unified Communications Manager. If SIP dial rules are not configured, KPML gets used. To increase the performance of Cisco Unified Communications Manager (increasing the number of calls that get processed), Cisco recommends that administrators configure SIP dial rules.

- Cisco Unified IP Phones 7940 and 7960 that are running SIP. These phones use the 7940_7960_OTHER dial rules pattern and do not support KPML. If the administrator does not configure a SIP dial plan for these phones, the user must wait a specified time before digits are sent to Cisco Unified Communications Manager for processing. This delays the actual call from being processed.

- Cisco Unified IP Phones 7905 and 7912 that are running SIP. These phones use the 7905_7912 dial rules pattern and do not support KPML. If the administrator does not configure a SIP dial plan for these phones, the user must wait a specified time before digits are sent to Cisco Unified Communications Manager for processing. This delays the actual call from being processed.

Although SIP dial rules are optional, if they are configured, you must add them to the phone that is running SIP by using the Phone Configuration window of Cisco Unified Communications Manager Administration. (If the administrator configures SIP dial plans, those dial plans must get associated with a phone device that is running SIP, so the dial plans get sent to the device configuration file.) Leave the SIP Dial Rules field in the Phone Configuration window set to <None> if you do not want dial rules applied to the Cisco Unified IP Phone.

After the administrator configures the SIP dial rule and applies it to the phone that is running SIP by pressing Reset, the database sends the TFTP server a notification, so it can build a new set of configuration files for the phone that is running SIP. The TFTP server notifies Cisco Unified Communications Manager about the new configuration file, and the updated configuration file gets sent to the phone. See Configure TFTP for Cisco Unified IP phones that run SIP, on page 107 for more information.

To accommodate Cisco Extension Mobility users, so they can use SIP dial rules, the administrator must configure the SIP dial rule on the phone that will allow extension mobility users to log on.

SRST does not support KPML; however, the phone that is running SIP will continue to use the Dial Rules that it received from Cisco Unified Communications Manager when it is in SRST mode.

Administrators use the SIP Dial Rules Configuration window to configure dial rule patterns and the parameters for the pattern.

SIP dial rule patterns

Two types of dial rule patterns exist in the SIP Dial Rules Configuration window:

- 7905_7912-Use this dial rule pattern for Cisco Unified IP Phones 7905 and 7912.

- 7940_7960_OTHER-Use this dial rule pattern for Cisco Unified IP Phones 7911, 7940, 7941, 7960, 7961, 7970, and 7971.
After the appropriate dial rule pattern gets chosen, the administrator configures the dial rule parameters for the dial rule pattern.

**Configure SIP dial rule parameters**

After the administrator defines the dial pattern, the SIP Dial Rule Information pane displays, so the administrator can configure the dial pattern parameters such as timeouts, buttons, or Private Line Automatic Ringdown (PLAR).

Ensure all pattern information has a name; for example, PLAR1 or 911. After you name the pattern information, you need to configure the parameters for the pattern. The SIP Dial Rules Configuration window displays an area for the pattern information. The administrator chooses the type of pattern parameter from a drop-down list box that displays on the configuration window. See Configure TFTP for Cisco Unified IP phones that run SIP, on page 107, for a description of the dial parameters.

These dial patterns get sent to the TFTP server, which creates the proper configuration file that contains the dial pattern information.

The following examples illustrate how to configure a dial rule for 911 and a pattern for any 4-digit extension beginning with the digit 2.

**Sample Dial Rule for 911 on Cisco Unified IP Phone 7905**

The administrator wants a dial rule pattern for 911 on the Cisco Unified IP Phone 7905.
Procedure

**Step 1**  Create a 7905 Steel SIP dial rule.

**Step 2**  Create a pattern called 911 for 7905.

**Step 3**  Enter a pattern description called 911.

**Step 4**  Enter 911 in the dial parameter value field.

**Figure 20: 05_12 911 Dial Rule Pattern**

Sample Dial Rule for Extension

The administrator wants a dial rule pattern for any 4-digit extension beginning with the digit 2 on a Cisco Unified IP Phone 7961.
Procedure

Step 1 Create a 7940_7960_OTHER SIP dial rule.
Step 2 Create a pattern called 4-digit extension.
Step 3 Enter a pattern description called SIP extension.
Step 4 Enter 2 followed by three dots (2...) in the dial parameter value field.

Private Line Automatic Ringdown (PLAR)

Configure a phone that is running SIP for Private Line Automatic Ringdown (PLAR), so when the user goes off hook (or the NewCall softkey or line key gets pressed), the phone immediately dials a preconfigured number. The phone user cannot dial any other number from the phone line that gets configured for PLAR. Because PLAR gets configured in Cisco Unified Communications Manager Administration as an empty pattern, it does not get associated with a device or line. To make the Cisco Unified IP Phone support PLAR, an empty pattern gets configured in the SIP Dial Rules for a specific line, and the dial rule then gets applied to the Cisco Unified IP Phone by using Phone Configuration in Cisco Unified Communications Manager Administration.

Note

Only Cisco Unified IP Phones 7940/41, 7960/61, and 7970/71 support PLAR for SIP.
URI dialing

Cisco Unified Communications Manager supports dialing using directory URIs for call addressing. Directory URIs look like email addresses and follow the username@host format where the host portion is an IPv4 address or a fully qualified domain name. A directory URI is a uniform resource identifier, a string of characters that can be used to identify a directory number. If that directory number is assigned to a phone, Cisco Unified Communications Manager can route calls to that phone using the directory URI. URI dialing is available for SIP and SCCP endpoints that support directory URIs.

This chapter contains the following topics:

- Set up URI dialing, page 211
- Directory URI format, page 213
- Directory URI provisioning, page 214
- Directory URI and directory number dial string interpretation, page 214
- Directory URI call routing, page 215
- Directory URI Replication with ILS, page 215
- Directory URI interoperability with VCS or third party system, page 216
- Directory URI LDAP integration, page 217
- Directory URI and directory number blended address, page 218
- Set up digit transformations for URI dialing, page 219
- Directory URI troubleshooting tips, page 221

Set up URI dialing

The following steps describe how to set up URI dialing in your network:
Procedure

**Step 1** Assign directory URIs to the users in your network.

**Step 2** Associate the directory URIs to directory numbers by assigning both a primary extension and phone to the users in your network.

**Step 3** Assign the default directory URI partition to an existing partition that is located in a calling search space by doing the following:

- In Cisco Unified CM Administration, choose **System > Enterprise Parameters**.
- For the Directory URI Alias Partition enterprise parameter, choose an existing partition that is in an existing calling search space.

**Step 4** Configure the SIP profiles in your network by configuring the following fields in the SIP Profile Configuration window:

- Configure a setting for the Dial String Interpretation drop-down list box and apply the setting for all the SIP profiles in your network.
- Check the **Use Fully Qualified Domain Name in SIP Requests** check box for all the SIP profiles in your network.

**Note** At this point, intracluster URI dialing is configured. The remaining steps are used to configure intercluster URI dialing.

**Step 5** For all the SIP trunks in your network, configure whether the network uses blended addressing by configuring the Calling and Connected Party Info Format drop-down list box in the Trunk Configuration window.

**Step 6** Set up ILS on all the clusters in your network.

**Step 7** Enable intercluster URI dialing with ILS by checking the **Exchange Directory URI Catalogs with Remote Clusters** check box in the Intercluster Directory URI Configuration window.

**Step 8** In the Intercluster Directory URI Configuration window, create a route string that remote clusters will use to route to this cluster.

**Step 9** Configure SIP route patterns that match the route strings for the remote clusters in your ILS network.

**Step 10** Associate the SIP route patterns that you created to an outbound SIP trunk or route list.

**Step 11** If you are connecting your ILS network to Cisco TelePresence Video Communications Server, or a third-party call control system, import directory URI catalogs from the other system into Cisco Unified Communications Manager.

**Step 12** If your deployment uses digit transformations to transform calling party directory numbers, configure calling party transformation patterns and apply them to the Inbound Call Settings for the phone or device pool. This configuration is used for intercluster calls.

**Step 13** If you applied digit transformation patterns in the previous step, configure calling party transformation patterns for the Outbound Call Settings for the phone or device pool. This configuration is used for intracluster calls.

**Related Topics**

- End user settings
- Directory URI and directory number dial string interpretation, on page 214
- Set up ILS network
Directory URI format

Directory URIs are alphanumeric strings consisting of a user and a host address separated by the @ symbol. Cisco Unified Communications Manager supports the following formats for directory URIs:

- user@domain (for example, joe@cisco.com)
- user@ip_address (for example, joe@10.10.10.1)

Cisco Unified Communications Manager supports the following formats in the user portion of a directory URI (the portion before the @ symbol):

- Accepted characters are a-z, A-Z, 0-9, !, $, %, &, *, _,-, ~, =, \, ?, ′, ‚, /.
- The user portion has a maximum length of 47 characters.
- The user portion accepts percent encoding from %2[0-9A-F] through %7[0-9A-F]. For some accepted characters, Unified CM automatically applies percent encoding. See below for more information on percent encoding.
- The user portion is case sensitive.

Cisco Unified Communications Manager supports the following formats in the host portion of a directory URI (the portion after the @ symbol):

- Supports IPv4 addresses or fully qualified domain names.
- Accepted characters are a-z, A-Z, 0-9, hyphens, and dots.
- The host portion cannot start or end with a hyphen.
- The host portion cannot have two dots in a row.
- Minimum of two characters.
- The host portion is not case sensitive.

Due to database restrictions, the Directory URI field has a maximum length of 254 characters.

---

**Note**
You can also enter a directory number in the user portion of a directory URI. However, Cisco Unified Communications Manager may treat the directory URI as a directory number depending on which Dial String Interpretation option you choose for the SIP Profile.

---

**Note**
For compatibility with third-party call control systems, we recommend using lower case for directory URIs.
Percent encoding of directory URIs

In the user portion of a directory URI, Unified CM automatically applies percent encoding to the following characters when the directory URI is saved in the database:

# % ^ ` {} | : " <> [ ] ' and spaces

When percent encoding is applied, the digit length of the directory URI increases. For example, if you input joesmith#@cisco.com (20 characters) as a directory URI, Cisco Unified Communications Manager stores the directory URI in the database as joe%20smith%23@cisco.com (24 characters). Due to database restrictions, Cisco Unified Communications Manager rejects any attempt to save a directory URI of greater than 254 characters.

Directory URI format exception for Bulk Administration

Within Cisco Unified CM Administration, you can enter directory URIs with embedded double quotes or commas. However, when you use Bulk Administration to import a CSV file that contains directory URIs with embedded double quotes and commas, you must use enclose the entire directory URI in double quotes and escape the embedded double quotes with a double quote. For example, the Jared,"Jerry",Smith@test.com directory URI must be input as "Jared,""Jerry",Smith@test.com" in the CSV file.

Directory URI provisioning

In Cisco Unified CM Administration, you can assign directory URIs in the local cluster in the following ways:

- **End User Configuration**—In End User Configuration, you can create end users and assign a phone, primary extension, and directory URI to that end user. Alternatively, if you synchronize your corporate LDAP directory with Cisco Unified Communications Manager, the LDAP data automatically populates for your end users. If the users in your LDAP directory have a phone, primary extension, and directory URI, they will automatically have directory URIs in Cisco Unified Communications Manager End User Configuration after the LDAP synchronization.

- **Directory Number Configuration**—In Directory Number Configuration, you can configure a directory number and associate a directory URI to that directory number. If that directory number is assigned to a phone, Cisco Unified Communications Manager allows you to dial that phone using the directory URI.

For both end user configuration and directory number configuration, you can also use Bulk Administration to import end users, directory URIs, directory numbers, and phones into Cisco Unified Communications Manager by bulk. See the *Cisco Unified Communications Manager Bulk Administration Guide* for more information.

For intracluster URI dialing, you must assign your directory URIs to a partition and calling search space. See **Set up URI dialing** for more information.

For intercluster URI dialing, Cisco Unified Communications Manager uses the Intercluster Lookup Service (ILS) to replicate directory URIs to other clusters in the ILS network. If ILS is configured to support intercluster directory URI Replication, each cluster sends out its catalog of known directory URIs to the other clusters in the ILS network. See **Directory URI Replication with ILS** for more information.

Directory URI and directory number dial string interpretation

Each phone that registers with Cisco Unified Communications Manager registers to its directory number. If a directory URI is associated with that directory number, users can dial that phone using the directory number
Directory URI call routing

Unified CM uses the following logic to route calls that are placed to a directory URI:

- Unified CM checks if the dial string is for a directory number. If the dial string is a directory number, Unified CM routes the call as a directory number.
- Else, Unified CM checks local calling search spaces and the local directory URI lookup table to see if the directory URI is in the local cluster. If the directory URI is on cluster, Unified CM routes the call to the appropriate endpoint.
- Else, Unified CM checks the URI catalogs that ILS maintains. If the directory URI is in a URI catalog, Unified CM finds the route string for the URI catalog and tries to match it to a SIP route pattern. If a matching SIP route pattern is found, Unified CM routes the call to the trunk that is associated with that route pattern.
- Else, Unified CM tries to match the host portion of the directory URI to a SIP route pattern. If the host portion matches a SIP route pattern, Unified CM routes the call to the SIP trunk that is associated to that route pattern.
- Else, Unified CM blocks the call.

Directory URI Replication with ILS

Cisco Unified Communications Manager uses the Intercluster Lookup Service (ILS) to support intercluster URI dialing. Using ILS, you can create large networks of remote Cisco Unified Communications Manager clusters. ILS also contains an optional directory URI replication feature that allows the clusters in an ILS network to replicate their directory URIs to the other clusters in the ILS network.

Directory URI Replication is configured individually for each cluster. Be aware that if you leave the feature disabled on a single cluster, it can affect other clusters in the network. For example, if directory URI replication is configured across the ILS network but is left disabled on a single hub cluster, the spoke clusters that are connected to that hub cannot exchange directory URIs with the rest of the ILS network.

To enable URI Replication in a cluster, check the Exchange Directory URIs with Remote Clusters check box that appears in Intercluster Directory URI Configuration. When this check box is checked, each cluster sends the following to the other clusters in the ILS network:

- All directory URIs known by the local cluster.
The local route string for each set of directory URIs.

Directory URI catalog types

Within an individual cluster, directory URIs can be categorized as follows:

- Local directory URIs—Directory URIs that are configured on the local system and which are saved in the local Unified CM database.
- Remote directory URIs—Directory URIs that were configured in another cluster and then replicated to this cluster.
- Imported Directory URI catalogs—Third party directory URIs that were manually imported into this cluster.
- Remote Imported Directory URI catalogs—Third party directory URIs that were manually imported into another cluster in the ILS network and then replicated to this cluster with ILS.

Local directory URIs are saved in the local Unified CM database. All other directory URIs are saved in CSV files that are maintained by ILS. When directory URI replication is enabled, ILS exchanges all types of directory URIs to the other clusters in the ILS network.

Route strings

In order to implement intercluster URI dialing, each cluster in the ILS network must be configured with a route string and SIP route patterns that match the route strings to an outbound trunk.

In many cases, the host portion of the directory URI is not granular enough for Unified CM to locate the cluster with the phone that is associated to that directory URI. Route strings provide additional information that Unified CM can use to route a call. When URI Replication is enabled, Unified CM exchanges directory URIs and the route string for the local cluster where that directory URI is saved.

You can create whatever route strings you want. For example, if you are joining clusters in San Jose and Paris, you could assign SanJose.USA.NorthAmerica and Paris.France.Europe as route strings for the two clusters. After you assign route strings for the various clusters, you must configure SIP route patterns that match the route strings for the next hop clusters in your ILS network. For example, in the San Jose cluster, you could configure a SIP route pattern that routes calls with a route string of Paris.France.Europe to an outbound SIP trunk.

If the San Jose cluster receives a call that is addressed to a directory URI from the Paris cluster, Unified CM checks the list of directory URIs maintained by ILS and pulls the directory URI and its local route string of Paris.France.Europe. If a SIP route pattern is configured that routes calls for Paris.France.Europe, Unified CM sends the call to the outbound trunk for that route pattern.

For more detail on configuring route strings, refer to the Cisco Unified Communications System SRND

Directory URI interoperability with VCS or third party system

Cisco Unified Communications Manager gives users with a supported endpoint the ability to place calls to alphanumeric URIs such as johnsmith@acme.com. The simplest way to route directory URI calls from a supported endpoint on Cisco Unified Communications Manager to an endpoint on a Cisco TelePresence Video Communications Server (VCS) or a third party call control system is to configure a domain-based SIP route pattern. For example, you can configure a SIP route pattern of acme.com to route calls addressed to the
acme.com domain out a SIP trunk that is configured for the Cisco TelePresence VCS or a third party call control system.

In situations where you have more than one Cisco TelePresence VCS or third party call control systems that use the same domain name, Cisco Unified Communications Manager can use the Intercluster Lookup Service (ILS) to provide URI dialing interoperability. For each Cisco TelePresence VCS, or third party system, you must manually create a csv file with the directory URIs that are registered to that call control system.

On a Cisco Unified Communications Manager cluster that is set up as a hub cluster in an ILS network, you can create an Imported directory URI catalog for each Cisco TelePresence VCS, or third party system, and assign a unique route string for each catalog. After you import the csv files into their corresponding Imported directory URI catalog, ILS replicates the imported directory URI catalog and route string to the other clusters in the ILS network.

On each Cisco Unified Communications Manager cluster, configure SIP Route Patterns that match the route string assigned to each Imported directory URI catalog in order to allow Cisco Unified Communications Manager to route directory URIs to an outbound trunk that is destined for the Cisco TelePresence VCS or third party system.

For more information on how to import directory URIs from a VCS into Cisco Unified Communications Manager, see the “Import directory URIs from a non-ILS system” procedure in the Intercluster Directory URI chapter of the Cisco Unified Communications Manager Administration Guide.

Cisco Unified Communications Manager also provides directory URI export functionality. You can export all directory URIs that were configured in the local cluster, including those that were imported from an LDAP directory, to a csv file that you can import into the other call control system. For more information on how to export directory URIs from Cisco Unified Communications Manager to a csv file, see the “Intercluster directory URI settings” section in the Intercluster Directory URI chapter of the Cisco Unified Communications Manager Administration Guide.

Related Topics

Import Directory URIs from a non-ILS system
Intercluster directory URI settings

Directory URI LDAP integration

Cisco Unified Communications Manager supports synchronization of directory URI fields in Cisco Unified CM Administration with data from a corporate LDAP directory.

When you synchronize with an LDAP directory, Unified CM automatically assigns the directory URI value that you choose from the LDAP directory as the primary directory URI for that end user. Even if you have already configured a directory URI as the primary directory URI for that end user’s primary extension, the LDAP value overrides the value that is configured in Cisco Unified CM Administration.

---

Note

The user portion of a directory URI is case sensitive. As a result, whatever case the directory URI has in the LDAP directory is the case in Cisco Unified Communications Manager. For example, if the directory URI value in LDAP is JOE@cisco.com, calls to joe@cisco.com in Cisco Unified Communications Manager will fail.
Directory URI and directory number blended address

Cisco Unified Communications Manager supports blended addressing of directory URIs and directory numbers. When blended addressing is enabled across the network, Cisco Unified Communications Manager inserts both the directory URI and the directory number of the sending party in outgoing SIP Invites, or responses to SIP Invites. The destination endpoint has the option of using either the directory URI or the directory number for its response—both will reach the same destination.

Cisco Unified Communications Manager uses the x-cisco-number tag in the SIP identity headers to communicate a blended address. When both a directory URI and directory number are available for the sending phone and blended addressing is enabled, Cisco Unified Communications Manager uses the directory URI in the From fields of the SIP message and adds the x-cisco-number tag with the accompanying directory number to the SIP identity headers. The x-cisco-number tag identifies the directory number that is associated with the directory URI.

For Cisco Unified Communications Manager to deliver a SIP message with blended addressing, the following conditions must be true:

- For all SIP trunks between the phones, the Calling and Connected Party Info Format drop-down list box must be set to Deliver URI and DN in connected party.
- Both a directory URI and a directory number must be configured for the phone that is sending the SIP message.
- The destination endpoint must support blended addressing.

For SIP trunks, blended addressing is enabled in the Trunk Configuration window of Cisco Unified CM Administration by setting the Calling and Connected Party Info Format drop-down list box to Deliver URI and DN in connected party. When Cisco Unified Communications Manager receives a SIP message with a blended address that is to be forwarded out a trunk, Cisco Unified Communications Manager checks whether blended addressing is enabled on the trunk before forwarding the message. If blended addressing is not enabled on the trunk, Cisco Unified Communications Manager removes the x-cisco-number tag before forwarding the SIP message.

For SIP lines, blended addressing is enabled by default. However, if a SIP message with a blended address is being forwarded out a SIP line to the destination endpoint, Cisco Unified Communications Manager checks whether the endpoint supports blended addressing. If the destination endpoint does not support blended addressing, Cisco Unified Communications Manager removes the x-cisco-number tag before forwarding the SIP message to the endpoint.

Blended addressing can be applied to the RPID, PAI, PPI, and Diversion headers.
Example 1
Bob at Cisco makes a call from extension 2100. The Calling and Connected Party Info Format field in the Trunk Configuration window is set to Deliver DN only in connected party. Blended addressing is not applied and the x-cisco-number tag is not added to the outgoing SIP message.
From:<sip:2100@10.10.10.1>
Remote-Party-ID:<sip:2100@10.10.10.1>;party=calling

Example 2
Jill at Cisco makes a call from extension 2030. The Calling and Connected Party Info Format field in the Trunk Configuration window is set to Deliver URI only in connected party. Blended addressing is not applied and the x-cisco-number tag is not added to the outgoing SIP message.
From:<sip:jill@cisco.com>
Remote-Party-ID:<sip:jill@cisco.com>;party=calling

Example 3
Alice at Cisco makes a call from extension 2000. The Calling and Connected Party Info Format field in the Trunk Configuration window is set to Deliver DN and URI in connected party. Blended addressing is applied. Cisco Unified Communications Manager adds the x-cisco-number tag to the SIP identity header.
From:<sip:alice@cisco.com>
Remote-Party-ID:<sip:alice@cisco.com;x-cisco-number=2000>;party=calling
John at Cisco extension 4003 receives Alice’s call, but John has his office phone set to forward calls to his home phone. If blended addressing is enabled, Cisco Unified Communications Manager adds a Diversion header with the x-cisco-number tag, and forwards the SIP INVITE to John’s home phone.
From:<sip:alice@cisco.com>
Diversion: <sip:john@cisco.com;x-cisco.number=4003>reason=no-answer
Remote-Party-ID:<sip:alice@cisco.com;x-cisco-number=2000>;party=calling

Set up digit transformations for URI dialing
If your network applies digit transformation patterns to calling party directory numbers and you are implementing URI dialing across clusters, you can apply calling party transformation patterns against the Inbound Call Settings of the phone or device pool. This is required because Cisco Unified Communications Manager cannot perform calling party transformations if the calling party transformation is applied based on the called party directory number or pattern.

For intercluster calls, you can apply a digit transformation pattern against a Calling Search Space (CSS) and apply that CSS transformation to the Inbound Call Settings for the phone or device pool. Before routing the call, whether the dialed number is a directory URI or a directory number, Cisco Unified Communications Manager applies the transformation pattern to the calling directory number.

For intracluster calls, if you don’t want the calling party transformation to be applied for calls that remain in the local cluster, you can also apply a CSS transformation pattern that strips the digits that were added by the Inbound Call Settings and apply that pattern to the Outbound Call Settings for the phone or device pool. For the device pool, the Calling Party Transformation CSS for outbound calls appears under Device Mobility Related Information.

To apply calling party digit transformations when URI dialing is implemented, do the following:
Procedure

**Step 1** In Cisco Unified CM Administration, choose **Call Routing > Class of Control > Partition** and create a new partition (for example, Change Calling Party XXXX to 8XXXXXXX).

**Step 2** Choose **Call Routing > Class of Control > Calling Search Space** and do the following:
- Create a calling search space (for example, Change Calling Party XXX to 8XXXXXXX).
- In the Available Partitions list box, add the newly created partition (for example, Change Calling Party XXXX to 8XXXXXXX).

**Step 3** In Cisco Unified CM Administration, choose **Call Routing > Transformation > Transformation Pattern > Calling Party Transformation Pattern**.
- Create a transformation pattern (for example, XXXX)
- Set the partition to the partition that you created in the previous steps (for example Change Calling Party XXXX to 8XXXXXXX).
- Set the Calling Party Transformation Mask to the desired mask (for example, 8265XXXX).

**Step 4** In Cisco Unified CM Administration, choose **Call Routing > Class of Control > Partition** and create a new partition (for example, Change Calling Party 8XXXXXXX to XXXX).

**Step 5** Choose **Call Routing > Class of Control > Calling Search Space** and do the following:
- Create a calling search space (for example, Change Calling Party 8XXXXXXX to XXXX).
- In the Available Partitions list box, add the newly created partition (for example, Change Calling Party 8XXXXXXX to XXXX).

**Step 6** In Cisco Unified CM Administration, choose **Call Routing > Transformation > Transformation Pattern > Calling Party Transformation Pattern**.
- Create a transformation pattern (for example, 8265XXXX)
- Set the partition to the partition that you created in the previous steps (for example, Change Calling Party 8XXXXXXX to XXXX).
- Set the Calling Party Transformation Mask to the desired mask (for example, XXXX).

**Step 7** To assign your transformation patterns to an individual phone, choose **Device > Phone** and apply the following settings to the phone:
- For patterns that apply to inbound settings, choose the CSS that contains the pattern from the Calling Party Transformation CSS drop-down list box that appears under Inbound Calls.
- For patterns that apply to outbound settings, choose the CSS that contains the pattern from the Calling Party Transformation CSS drop-down list box that appears under Outbound Calls.

**Step 8** Click **Save**.

**Note** You can also apply the digit transformation patterns to a device pool by choosing **System > Device Pool** from Cisco Unified CM Administration. For device pool configuration, the Calling Party Transformation CSS for outbound calls appears under Device Mobility Related Information.
Directory URI troubleshooting tips

This section describes some basic troubleshooting scenarios for URI dialing.

Directory URI has been dialed, but the call fails

Check the following:

• The user portion of a directory URIs is case sensitive. Check that the dialed directory URI and the provisioned directory URI use the same case.

• Check the partition, directory URI partition, and calling search space of the called party. For intracluster calls, make sure the destination phone is in the same calling search space.

• Check the Dial String Interpretation policy against the dialed directory URI. If the implemented dial string interpretation policy interprets the directory URI as a directory number, Cisco Unified Communications Manager may not be able to route the call.

• Use the Dialed Number Analyzer tool to determine if Cisco Unified Communications Manager can route a call to that directory URI.

Note

The Dialed Number Analyzer can only be used to test routing for intracluster calls.

Directory URI has been dialed, but the call display shows a directory number

Check the following:

• Check to see whether the phone model supports blended addressing. If the phone model does not support blended addressing, the directory number is displayed.

• Check to see whether the Alerting Name is configured. The Alerting Name overrides the dial string.

• If the incorrect display is on the called phone, check to see whether the calling phone has a primary directory URI configured.
PART IV

Directory user configuration and credential policy

- Directory overview, page 225
- Application users and end users, page 233
- Credential policy, page 239
CHAPTER 20

Directory overview

This chapter provides information about directories which comprise specialized databases that are optimized for a high number of reads and searches and occasional writes and updates. Directories typically store data that does not change often, such as employee information, user privileges on the corporate network, and so on.

Because directories are extensible, you can modify and extend the type of information that is stored in them. The term directory schema refers to the type of stored information and the rules that it obeys. Many directories provide methods for extending the directory schema to accommodate information types that different applications define. This capability enables enterprises to use the directory as a central repository for user information.

The Lightweight Directory Access Protocol (LDAP) provides applications with a standard method for accessing and potentially modifying the information that is stored in the directory. This capability enables companies to centralize all user information in a single repository that is available to several applications with a reduction in maintenance costs through the ease of adds, moves, and changes.

This chapter covers the main principles for synchronizing Cisco Unified Communications Manager with a corporate LDAP directory. The chapter also discusses the administrator choice not to synchronize with a corporate LDAP directory and the consequences of that choice of configuration. The chapter also summarizes considerations for providing Cisco Unified Communications endpoints, such as Cisco Unified IP Phones and Cisco IP Softphone, with access to a corporate LDAP directory.

The following list summarizes the changes in directory functionality from previous releases of Cisco Unified Communications Manager:

- Decoupling the directory component from Cisco Unified Communications Manager ensures high Cisco Unified Communications Manager availability independent of the corporate directory.
- Cisco Unified Communications Manager and related applications store all application data in the local database instead of in an embedded directory. The embedded directory gets removed, and Cisco Unified Communications Manager supports synchronization with the customer directory.

- Configure LDAP directory, page 226
- Cisco Unified Communications Manager and the corporate LDAP directory, page 227
- Directory access, page 228
- DirSync service, page 228
- Authentication, page 229
Configure LDAP directory

If you want to do so, you can add users from your corporate directory to the Cisco Unified Communications Manager database by synchronizing the user data to the database. Cisco Unified Communications Manager allows synchronization from the following directories to the database:

- Microsoft Active Directory 2000
- Microsoft Active Directory 2003
- Microsoft Active Directory 2008
- Microsoft Active Directory Application Mode 2003
- Microsoft Lightweight Directory Services 2008
- iPlanet Directory Server 5.1
- Sun ONE Directory Server 5.2
- Sun ONE Directory Server 6.x
- OpenLDAP 2.3.39
- OpenLDAP 2.4

Note

Microsoft Active Directory Application Mode support is limited to those directory topologies already supported with a native Active Directory connection. No additional topologies, such as multi-forest, multi-tree single forest, or global catalog are supported.

Cisco Unified Communications Manager supports the following types of synchronization:

- Automatic synchronization, which synchronizes the data at regular intervals.
- Manual synchronization, which allows forcing the synchronization.
- Stop synchronization, which stops the current synchronization. If synchronization is in progress, check for agreement.

The general steps and guidelines for configuring LDAP directory information are as follows.

Procedure

Step 1 Activate the DirSync service to synchronize with the customer corporate LDAP directory.
Step 2  Access the LDAP System Configuration window to configure LDAP system settings.
Step 3  If you want to use LDAP filters, access the LDAP Filter Configuration window to create LDAP filters.
Step 4  Access the LDAP Directory window to configure LDAP directory settings.
Step 5  Access the LDAP Authentication window to configure LDAP authentication settings.
Step 6  After the LDAP user gets synchronized in Cisco Unified Communications Manager, you must manually create the user in Cisco Unity Connection Administration. To manually create the user, perform one of the following tasks:

- Import the user into Cisco Unity Connection by configuring Cisco Unity Connection Administration, as described in the User Moves, Adds, and Changes Guide for Cisco Unity Connection.

- Choose User Management > End User in Cisco Unified Communications Manager Administration and create the Cisco Unity Connection mailbox.

User Moves, Adds, and Changes Guide for Cisco Unity Connection

---

Cisco Unified Communications Manager and the corporate LDAP directory

In Cisco Unified Communications Manager Administration, you can access directory information about end users from the End User Configuration window (User Management > End User). If you do not enable LDAP synchronization, you use this window to add, update, and delete user information such as user ID, password, and device association. If you enable LDAP synchronization, you cannot add an end user, delete an end user, or change some existing user information, including user IDs, in the End User Configuration windows.

Applications and Services That Use the Database

The following Cisco Unified Communications Manager applications and services use the database for user and other types of information:

- Bulk Administration Tool (BAT)
- Cisco Unified Communications Manager Auto-Register Phone Tool
- AXL
- Cisco Extension Mobility
- Cisco Unified CM User Options
- Cisco Conference Connection
- CTIManager
- Cisco Unified Communications Manager CDR Analysis and Reporting
- Cisco Unified Communications Manager Assistant
- Cisco Customer Response Solutions (CRS)
- Cisco Emergency Responder (CER)
Directory access

The following definition applies throughout this chapter:

- Directory access refers to the ability of Cisco Unified Communications endpoints, such as Cisco Unified IP Phones and Cisco IP Softphone, to access a corporate LDAP directory.

![Figure 22: Directory Access for Cisco Unified Communications Endpoints]

The previous figure illustrates directory access as it is defined in this chapter. In this example, a Cisco Unified IP Phone gets access. The client application performs a user search against an LDAP directory, such as the corporate directory of an enterprise, and receives several matching entries. The Cisco Unified IP Phone user can then select one entry and use it to dial the corresponding person from the Cisco Unified IP Phone.

---

**Note**

Directory access, as defined here, involves only read operations on the directory and does not require that you make any directory schema extensions or other configuration changes.

DirSync service

The Cisco Unity Connection directory comes from Cisco Unified Communications Manager; that is, components in Cisco Unity Connection synchronize directory updates from Cisco Unified Communications Manager to Cisco Unity Connection. If you enable LDAP synchronization and activate the DirSync service in Cisco Unified Serviceability, the DirSync service in Cisco Unified Communications Manager synchronizes corporate directory data for Cisco Unified Communications Manager and Cisco Unity Connection to the Cisco Unified Communications Manager database.

After you activate the DirSync service in Cisco Unified Serviceability, you configure LDAP related information in the following windows in Cisco Unified Communications Manager Administration:

- LDAP System Configuration (System > LDAP System)
- Find and List LDAP Directories (System > LDAP > LDAP Directory)
DirSync allows you to synchronize the data from corporate directories to Cisco Unified Communications Manager. For information about which directories are supported for synchronization, see the Configure LDAP directory, on page 226.

When you configure a user in the corporate directory, ensure that you configure a last name for the user. After you configure LDAP synchronization in Cisco Unified Communications Manager Administration, users without last names in the corporate directory do not synchronize with the Cisco Unified Communications Manager database. No error displays in Cisco Unified Communications Manager Administration, but the log file indicates which users did not synchronize.

DirSync allows the following options:

- Automatic synchronization, which synchronizes the data at regular intervals.
- Manual synchronization, which allows forcing the synchronization.
- Stop synchronization, which stops the current synchronization. If synchronization is in progress, check for agreement.

When directory synchronization is enabled, Cisco Unified Communications Manager Administration cannot update any user information that is synchronized from the customer corporate directory.

**Configure DirSync service parameters**

You can configure service parameters for the DirSync service. Choose **System > Service Parameters** in Cisco Unified Communications Manager Administration. In the window that displays, choose a server in the Server drop-down list box. Choose the Cisco DirSync service in the Service drop-down list box. The Service Parameter Configuration window allows configuration of the DirSync service parameters.

For specific information on how to activate the DirSync service, see the Cisco Unified Serviceability Administration Guide.

**Authentication**

The authentication process verifies the identity of the user by validating the user ID and password/PIN before granting access to the system. Verification takes place against the Cisco Unified Communications Manager database or the LDAP corporate directory.

You can only configure LDAP authentication if you enable LDAP synchronization.
When both synchronization and LDAP authentication are enabled, the system always authenticates application users and end user PINs against the Cisco Unified Communications Manager database. End user passwords get authenticated against the corporate directory; thus, end users need to use their corporate directory password.

When only synchronization is enabled (and LDAP authentication is not enabled), end users get authenticated against the Cisco Unified Communications Manager database. In this case, the administrator can configure a password in the End User Configuration window in Cisco Unified Communications Manager Administration.

Use the Cisco Unified Communications Manager database

Two options exist for using directory information:

- To use the Cisco Unified Communications Manager database for users, create users in the End User Configuration window to add to the database (password, names, device association, and so forth). Authentication takes place against the information that is configured in Cisco Unified Communications Manager Administration. End users and administrators can make password changes if this method is used. This method does not entail LDAP synchronization.

  The Cisco Unity Connection directory comes from Cisco Unified Communications Manager; that is, components in Cisco Unity Connection synchronize directory updates from Cisco Unified Communications Manager to Cisco Unity Connection.

- To use the Corporate LDAP directory, the following steps must take place:
  - For users to use their LDAP corporate directory passwords, you must configure LDAP authentication (System > LDAP > LDAP Authentication).
  - You cannot configure LDAP authentication unless you first configure LDAP synchronization. Doing so blocks further end user configuration in Cisco Unified Communications Manager Administration.
  - After the LDAP user synchronizes to Cisco Unified Communications Manager, you must manually create the user for Cisco Unity Connection.

Tip

Keep in mind that configuring authentication is optional. If authentication is not enabled, administrators and end users have two passwords, a corporate directory password and a Cisco Unified Communications Manager password.

Directory access for Cisco Unified Communications endpoints

The guidelines in this section apply regardless of whether Cisco Unified Communications Manager or other Cisco Unified Communications applications have been synchronized with a corporate directory. The end-user perception in both cases remains the same because the differences affect only how applications store their user information and how such information is kept consistent across the network.

The following sections summarize how to configure corporate directory access to any LDAPv3-compliant directory server for XML-capable phones such Cisco Unified IP Phones 7940, 7960, and so on.
Cisco IP Softphone, Release 1.2 and later, includes a built-in mechanism to access and search LDAP directories, as does the Cisco IP Communicator. See the product documentation for details on how to configure this feature.

**Note**

Directory Access for Cisco Unified IP Phones

XML-capable Cisco Unified IP Phones, such as 7940 and 7960, can search a corporate LDAP directory when a user presses the Directories button on the phone. The IP phones use HyperText Transfer Protocol (HTTP) to send requests to a web server. The responses from the web server must contain some specific Extensible Markup Language (XML) objects that the phone can interpret and display. In the case of a corporate directory search, the web server operates as a proxy by receiving the request from the phone and translating it into an LDAP request, which is in turn sent to the corporate directory server. After the response is encapsulated in the appropriate XML objects, the response gets interpreted and sent back to the phone.

This figure illustrates a deployment where Cisco Unified Communications Manager has not been synchronized with the corporate directory. In this scenario, the message exchange does not involve Cisco Unified Communications Manager.

*Figure 23: Message Exchange for Cisco Unified IP Phone Corporate Directory Access Without Directory Synchronization*

You can configure the proxy function that the web server provided by using the Cisco Unified IP Phone Services Software Development Kit (SDK) version 2.0 or later, which includes the Cisco LDAP Search Component Object Model (COM) server.

In addition, directory access for Cisco Unified IP Phones includes the following characteristics:

- The system supports all LDAPv3-compliant directories.
- Cisco Unified Communications Manager user preferences (speed dials, call forward all, personal address book) do not get synchronized with the corporate LDAP directory. Therefore, users have a separate login and password to access the Cisco Unified CM User Options window.
Application users and end users

This chapter provides information about the Application User Configuration window and the End User Configuration window in Cisco Unified Communications Manager Administration which allow the administrator to add, search, display, and maintain information about Cisco Unified Communications Manager application users and end users. This chapter describes the options for managing user information.

- Manage application user and end user configuration, page 233
- Application users, page 234
- End users, page 235
- Credential management, page 236
- User and application profiles, page 236
- Device association, page 236
- Cisco Unified Mobility for end users, page 237
- Cisco Extension Mobility profiles, page 238
- Cisco IP softphone profiles, page 238

Manage application user and end user configuration

The Application User Configuration window and the End User Configuration window in Cisco Unified Communications Manager Administration allow you to add, search, display, and maintain information about Cisco Unified Communications Manager application users and end users.

The general steps and guidelines for managing application user and end user information is as follows.
Procedure

Step 1 Search for an application user.
Step 2 Add an application user as needed.
Step 3 Manage application user credentials.
Step 4 Search for an end user.
Step 5 Add an end user as needed.
Step 6 Configure application profiles for end users.
Step 7 Manage end user credentials.

Application users

Application user configuration allows updates to the application users that are associated with Cisco Unified Communications Manager. By default, Cisco Unified Communications Manager Administration includes these application users:

- CCMAadministrator
- CCMSysUser
- CCMQRTSecureSysUser
- CCMQRTSysUser
- IPMASecureSysUser
- IPMASysUser
- WDSecureSysUser
- WDSysUser
- TabSyncSysUser
- CUCService

Installation requires you to configure an administrator login and password for the system. You cannot delete these default application users or the administrator user that you create at install, but you can change their passwords and modify the lists of devices that they control.

Tip

Ensure that you do not lose the password that you created during installation.
Administrator users in the Standard CCM Super Users group can access all administrative applications in the Cisco Unified Communications Manager Administration navigation menu (Cisco Unified Communications Manager Administration, Cisco Unified Serviceability, and Cisco Unified Reporting) with a single sign-on to one of the applications.

You set the default Administrator username and password during Cisco Unified Communications Manager installation. You can change the administrator password or set up a new administrator account in the Application User Configuration window in Cisco Unified Communications Manager Administration.

To configure application user information in Cisco Unified Communications Manager, use the User Management > Application User menu option in Cisco Unified Communications Manager Administration.

Note
To configure this user for Cisco Unity or Cisco Unity Connection, you configure the application user in Cisco Unified Communications Manager Administration; then, configure any additional settings for the user in Cisco Unity or Cisco Unity Connection Administration.

End users

You can add end users to the Cisco Unified Communications Manager database, or you can use the corporate LDAP directory. If you use the corporate directory for authentication, end users use their LDAP directory passwords; you cannot change these passwords. You can, however, configure and change end user PINs.

Note
If your system uses LDAP authentication, you must configure end user default credentials immediately after installation, or logins will fail. The system does not support empty (null) credentials.

You can add new end users through Cisco Unified Communications Manager Administration only when synchronization with the corporate LDAP server is disabled. When synchronization is disabled, you can add new users, and you can change the settings of existing users, including the user ID. If synchronization is enabled, you cannot add users, delete users, or change existing user IDs. You can, however, change all other settings for existing end users in the End User Configuration window.

To check whether LDAP synchronization is enabled, choose System > LDAP > LDAP System in Cisco Unified Communications Manager Administration. If the Enable Synchronizing from LDAP Server check box is checked, you know that synchronization is enabled.

To configure end user information, choose User Management > End User in Cisco Unified Communications Manager Administration.

You can use the End User, Phone, DN, and LA Configuration window to add a new user and a new phone at the same time. You can associate a directory number and line appearance for the new end user by using the same window. To access the End User, Phone, DN, and LA Configuration window, choose User Management > User/Phone Add.

Note
The End User, Phone, DN, and LA Configuration window only allows adding a new end user and a new phone. The window does not allow entry of existing end users or existing phones.
To configure this user for Cisco Unity or Cisco Unity Connection, you configure the end user in Cisco Unified Communications Manager Administration; then, configure any additional settings for the user in Cisco Unity or Cisco Unity Connection Administration.

### Credential management

When you configure an application or end user, you can add or change login credentials (password or PIN) in the user configuration window.

After the user gets added to the database, you can manage these credentials in the Credential Configuration for window, which you access with the Edit Credentials button in the End User or Application User Configuration window. For example, you can block the user from changing the password, or you can require the user to change the password at the next login.

You can also view lockout events and reset a lockout for a password or PIN for the user. Authentication events get updated in the window according to the credential policy that you assigned to this user.

The Credential Configuration window also provides an option to change the user credential policy assignment. To manage credentials for individual users, or for more information about credential policies, see Credential policy, on page 239.

### User and application profiles

After you add a new application or end user, you can assign a CAPF profile with the End User CAPF Profile or the Application User CAPF Profile menu options. Cisco Unified Communications Manager uses the CAPF profile to authenticate application or end user certificate downloads from the CAPF server. JTAPI / TSP or CTI applications use this certificate to establish a secure connection with Cisco CTIManager.

After you assign the profile, the CAPF Information pane in the user configuration window displays the assigned profile and allows you to update the settings. For general information about CAPF profiles, see the Credential policy, on page 239 section.

After you add a new end user, options in the Extension Mobility pane allow you to configure extension mobility profiles. These profiles allow each end user to personalize Cisco Extension Mobility.

### Device association

Associating devices to an application user or to an end user gives the user control over specified devices. Application users and end users control some devices, such as phones. When application users or end users have control of a phone, they can control certain settings, such as speed dial and call forwarding, for that phone.

#### Device association for application users

Use the Device Information portion of the Application User Configuration window to associate devices with an existing application user. The Available Devices pane lists the devices that are available for association with an application user. The Available Devices pane lists devices by device name. To search for additional
devices to associate with an application user, use the **Find more Phones**, **Find more Route Points**, and **Find more Pilot Points** buttons. Each button opens a popup window where you can limit the list of devices by entering search criteria based on all or part of the device name, description, or other parameter. To limit the list of available devices to a specific selection, enter the criteria by which you want to search by using the following methods:

- Choose a search parameter, such as device name, description, or directory number.
- Choose the comparison operator, such as begins with.
- Enter search text.

For example, to list all extensions that begin with “5,” you would choose Directory Number begins with and then enter 5 in the text box.

After you have specified the search criteria to display devices, all matching, available devices display in the Search Results. You can navigate the list by using the buttons at the bottom of the window.

You can associate one or more devices to the application user by checking that check box next to that device. If a device has multiple extensions that are associated with it, each line extension displays in the list. You need to choose only one line extension to choose all the lines that are associated with that device.

### Device association for end users

Use the Device Associations portion of the End User Configuration window to associate devices with an existing end user. The Controlled Devices pane lists the devices that are already associated with an end user. The Controlled Devices pane lists devices by device name. To search for additional devices to associate with an end user, use the **Device Association** button. This button opens the User Device Association window where you can limit the list of devices by entering search criteria based on all or part of the device name or description. To limit the list of available devices to a specific selection, enter the criteria by which you want to search by using the following methods:

- Choose a search parameter, such as device name or description.
- Choose the comparison operator, such as begins with.
- Enter search text.

After you have specified the search criteria to display devices, all matching, available devices display in the Device association for (this end user) portion of the User Device Association window. You can navigate the list by using the buttons at the bottom of the window.

You can associate one or more devices to the end user by checking that check box next to that device. If a device has multiple extensions that are associated with it, each line extension displays in the list. You need to choose only one line extension to choose all the lines that are associated with that device.

### Cisco Unified Mobility for end users

In the End User Configuration window, you can enable Mobile Connect and Mobile Connect Access for the user. Checking the Enable Mobility check box in the End User Configuration window triggers licensing to consume device license units for Mobile Connect, and assigning a device to the user specifically for Cisco Unified Mobility controls the number of device license units that are consumed for Cisco Unified Mobility.

In the End User Configuration window, you can also configure the maximum time that is permitted to pass before the user must pick up a call that is transferred from the mobile phone to a desktop phone. Likewise,
you can configure the maximum number of phones to which the user is permitted to transfer calls from the
desktop phone.

The End User Configuration window lists the remote destination profiles that are configured for the end user.

**Cisco Extension Mobility profiles**

Use Cisco Extension Mobility to configure a Cisco Unified IP Phone to appear temporarily as a user phone. The user can log in to a phone, and the user extension mobility profile (including line and speed-dial numbers) resides on the phone. This feature applies primarily in environments where users do not get permanently assigned to physical phones.

User device profiles and device profile defaults support the Cisco Extension Mobility feature. The user device profile includes the following information:

- Device Profile Information-Includes Device Type, User Device Profile Name, Description, User Hold Audio Source, and User Locale.
- Phone Button Information-Includes Phone Button Template for the device type.
- Softkey Template Information-Includes list of available softkey templates.
- Expansion Module Information-Includes Cisco Unified IP Phone add-on modules such as the Cisco Unified IP Phone 7914 Expansion Module.
- Multilevel Precedence and Preemption Information-Includes MLPP domain, indication, and preemption settings.
- Logged-Out Default Profile Information-Includes Log In User ID

An authentication scheme authenticates the user. The workflow engine sends an XML string through an HTTP post request to the Login Service. The string contains the following items:

- User name and password of the login application
- Device name that is based on the MAC address of the device on which the user wants their profile to reside

A dialog prompt displays on the device of the user.

**Cisco IP softphone profiles**

You can associate a device (line) to a user as a Cisco IP Softphone. This enables users to use their desktop PC to place and receive telephone calls and to control an IP telephone.
Credential policy

This chapter provides information about Cisco Unified Communications Manager credential policy which authenticates user login credentials before allowing system access. To help secure user accounts, you can specify settings for failed logon attempts, lockout durations, password expirations, and password requirements in Cisco Unified Communications Manager Administration. These authentication rules form a credential policy.

Credential policies apply to application users and end users. You assign a password policy to end users and application users and a PIN policy to end users. The Credential Policy Default Configuration lists the policy assignments for these groups.

At installation, Cisco Unified Communications Manager assigns a static Default Credential Policy to user groups. It does not provide default credentials. The Credential Policy Default Configuration window in Cisco Unified Communications Manager Administration provides options to assign new default policies and to configure new default credentials and credential requirements for users.

Note

The system does not support empty (null) credentials. If your system uses LDAP authentication, you must configure end user default credentials immediately after installation, or logins fail.

When you add a new user to the Cisco Unified Communications Manager database, the system assigns the default policy. You can change the assigned policy and manage user authentication events with the Edit Credentials button in the user configuration window.

- Configure credential policy, page 240
- Credential policy and authentication, page 240
- Credential caching, page 241
- BAT administration, page 241
- JTAPI/TAPI support, page 241
- Credential history, page 241
- Authentication events, page 242
Configure credential policy

Cisco Unified Communications Manager authenticates user login credentials before allowing system access. To help secure user accounts, you can specify settings for failed logon attempts, lockout durations, password expirations, and password requirements in Cisco Unified Communications Manager Administration. These authentication rules form a credential policy.

Credential policies apply to application users and end users. You assign a password policy to end users and application users and a PIN policy to end users. The Credential Policy Default Configuration lists the policy assignments for these groups.

At installation, Cisco Unified Communications Manager assigns a static Default Credential Policy to user groups. It does not provide default credentials. The Credential Policy Default Configuration window in Cisco Unified Communications Manager Administration provides options to assign new default policies and to configure new default credentials and credential requirements for users.

**Note**
The system does not support empty (null) credentials. If your system uses LDAP authentication, you must configure end user default credentials immediately after installation, or logins fail.

When you add a new user to the Cisco Unified Communications Manager database, the system assigns the default policy. You can change the assigned policy and manage user authentication events with the Edit Credentials button in the user configuration window.

The general steps and guidelines for configuring credential policies are as follows.

**Procedure**

**Step 1** Use the Credential Policy Configuration window to configure a credential policy other than the default policy.

**Step 2** Use the Credential Policy Default windows to assign a new credential policy and configure a common password for an account type.

**Step 3** To manage or monitor the credential configuration for individual users, click the **Edit Credential** link in the user configuration window.

**Credential policy and authentication**

The authentication function in Cisco Unified Communications Manager authenticates users, updates credential information, tracks and logs user events and errors, records credential change histories, and encodes/decodes or encrypts/decrypts user credentials for data storage.

The system always authenticates application user passwords and end user PINs against the Cisco Unified Communications Manager database. The system can authenticate end user passwords against the corporate directory or the Cisco Unified Communications Manager database.

If your system is synchronized with the corporate directory, either the authentication function in Cisco Unified Communications Manager or LDAP can authenticate the password.
• With LDAP authentication enabled, user passwords and credential policies that are configured in Cisco Unified Communications Manager Administration do not apply. These defaults get applied to users that are created with directory synchronization (DirSync service).

• When LDAP authentication is disabled, the system authenticates user credentials against the Cisco Unified Communications Manager database. With this option, administrators can assign credential policies, manage authentication events, and administer passwords. End users can change passwords and PINs at the phone user pages.

See the Directory overview, on page 225 for more information about LDAP authentication.

Credential policies do not apply to OS users or CLI users. These administrators use standard password verification procedures that the OS supports. See the Cisco Unified Communications Operating System Administration Guide for information about OS login procedures.

**Credential caching**

To improve performance, administrators can configure the enterprise parameter “Enable Caching” to True. The parameter enables Cisco Unified Communications Manager to use cached credentials for up to 2 minutes. This eliminates the need for Cisco Unified Communications Manager to perform a database lookup or invoke a stored procedure for every single login request, thereby increasing system efficiency. An associated credential policy does not get enforced until the caching duration expires.

This setting applies to all Java applications that invoke user authentication. Setting the enterprise parameter to False turns off caching, so the system does not use cached credentials for authentication. The system ignores this setting for LDAP authentication. Credential caching requires a minimal amount of additional memory per user.

**BAT administration**

The Bulk Administration Tool (BAT) allows administrators to define common credential parameters, such as passwords and PINs, for a group of users in the BAT User Template. When you first create a user template, all the users get assigned the static Default Credential Policy.

**JTAPI/TAPI support**

Because Cisco Unified Communications Manager Java Telephony Applications Programming Interface (JTAPI) and Telephony Applications Programming Interface (TAPI) support the credential policies that are assigned to application users, developers must create applications that react to the password expiration, PIN expiration, and lockout return codes for credential policy enforcement.

Applications use an API to authenticate with the database or corporate directory, regardless of the authentication model that an application uses.

**Credential history**

After a user is configured in the database, the system stores a history of user credentials in the database to prevent a user from entering previous credentials when the user is prompted to change credentials.
Authentication events

You can monitor and manage authentication activity for a user at the user Credential Configuration page, which is accessed with the Edit Credentials button in the user configuration windows. The system shows the most current authentication results, such as last hack attempt time, and counts for failed logon attempts.

See Directory overview, on page 225 for more information.

The system generates log file entries for the following credential policy events:

- Authentication success
- Authentication failure (bad password or unknown)
- Authentication failure due to
  - Administrative lock
  - Hack lock (failed logon lockouts)
  - Expired soft lock (expired credential)
  - Inactive lock (credential not used for some time)
  - User must change (credential set to user must change)
  - LDAP inactive (switching to LDAP authentication and LDAP not active)
- Successful user credential updates
- Failed user credential updates

Note

If you use LDAP authentication for end user passwords, LDAP tracks only authentication successes and failures.

All event messages contain the string “ims-auth” and the userid that is attempting authentication.

You can view log files with the Cisco Unified Real-Time Monitoring Tool. You can also collect captured events into reports.
Media resources

- Media resource management, page 245
- Annunciator, page 257
- Conference bridges, page 265
- Transcoders, page 287
- Music on hold, page 293
- Media Termination Points, page 295
- Cisco DSP resources for transcoding conferencing and MTP, page 303
Media resource management

Cisco Unified Communications functionality requires the use of media resources. Media resources provide services such as annunciator, transcoding, conferencing, music on hold, and media termination.

The media resource manager enhances Cisco Unified Communications Manager features by making Cisco Unified Communications Manager more readily able to deploy annunciator, media termination point, transcoding, conferencing, and music on hold services.

- Configure media resource group and media resource group list, page 245
- Media resources overview, page 246
- Trusted relay point, page 248
- Media resource groups, page 252
- Media resource group lists, page 253
- Dependency records, page 255

Configure media resource group and media resource group list

Cisco Unified Communications Manager media resource groups and media resource group lists provide a way to manage resources. Use these resources for conferencing, transcoding, media termination, and music on hold (MOH).

Media resource groups define logical groupings of media servers. You can associate a media resource group with a geographical location or a site as desired. You can also form media resource groups to control the usage of servers or the type of service (unicast or multicast) that is desired.

Media resource group lists specify a list of prioritized media resource groups. An application can select required media resources from among the available resources according to the priority order that is defined in the media resource group list. Media resource group lists, which are associated with devices, provide media resource group redundancy.

The following steps describe how to configure media resource groups and media resource group lists.
Media resources overview

Media resource management provides access to media resources for all Cisco Unified Communications Managers in a cluster. Every Cisco Unified Communications Manager contains a software component called a media resource manager. The media resource manager locates the media resource that is necessary to connect media streams to complete a feature.

The media resource manager manages the following media resource types:

- Music On Hold (MOH) server
- Unicast conference bridge (CFB)
- Media termination point (MTP)
- Transcoder (XCODE)
- Annunciator (ANN)
- Trusted relay point (TRP)

The following reasons explain why resources are shared:

- To allow both hardware and software devices to coexist within a Cisco Unified Communications Manager
- To enable Cisco Unified Communications Manager to share and access resources that are available in the cluster
- To enable Cisco Unified Communications Manager to do load distribution within a group of similar resources
- To enable Cisco Unified Communications Manager to allocate resources on the basis of user preferences

Initialization of the Cisco Unified Communications Manager creates a media resource manager. Each media termination point, music on hold, transcoder, conference bridge, and annunciator device that is defined in the database registers with the media resource manager. The media resource manager obtains a list of provisioned devices from the database and constructs and maintains a table to track these resources. The media resource manager uses this table to validate registered devices. The media resource manager keeps track of the total devices that are available in the system, while also tracking the devices that have available resources.

When a media device registers, Cisco Unified Communications Manager creates a controller to control this device. After the device is validated, the system advertises its resources throughout the cluster. This mechanism allows the resource to be shared throughout the cluster.

Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Create a media resource group.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Assign device to the media resource group. (Order has no significance.)</td>
</tr>
<tr>
<td>Step 3</td>
<td>Create a media resource group list. (Order has significance.)</td>
</tr>
<tr>
<td>Step 4</td>
<td>Assign a media resource group to a media resource group list.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Assign a media resource group list to a device or device pool.</td>
</tr>
</tbody>
</table>
Resource reservation takes place based on search criteria. The given criteria provide the resource type and the media resource group list. When the Cisco Unified Communications Manager no longer needs the resource, resource deallocation occurs. Cisco Unified Communications Manager updates and synchronizes the resource table after each allocation and deallocation.

The media resource manager interfaces with the following major components:

- Call control
- Media control
- Media termination point control
- Unicast bridge control
- Music on hold control
- Annunciator control
- Trusted relay point

**Call Control**

Call control software component performs call processing, including setup and tear down of connections. Call control interacts with the feature layer to provide services like transfer, hold, conference, and so forth. Call control interfaces with the media resource manager when it needs to locate a resource to set up conference call and music on hold features.

**Media Control**

Media control software component manages the creation and teardown of media streams for the endpoint. Whenever a request for media to be connected between devices is received, depending on the type of endpoint, media control sets up the proper interface to establish a stream.

The media layer interfaces with the media resource manager when it needs to locate a resource to set up a media termination point or transcoding.

**Media Termination Point Control**

Media termination point (MTP) provides the capability to bridge an incoming H.245 stream to an outgoing H.245 stream. MTP maintains an H.245 session with an H.323 endpoint when the streaming from its connected endpoint stops. MTP supports the G.711 and G.729 codecs. MTP can also transcode G.711 a-law to mu-law. MTP also enables Early Offer on SIP trunks and Fast Start on H.323 trunks. MTPs also get dynamically inserted to perform DTMF transport translation for endpoints that do not support a common DTMF transport method.

The Media Resource Manager (MRM) provides resource reservation of transcoders within a Cisco Unified Communications Manager cluster. Transcoders comprise another media resource type that is hardware based and uses Digital Signal Processing (DSP). DSP resources also support MTP functionality. Cisco Unified Communications Manager supports simultaneous registration of both the MTP and transcoder and concurrent MTP and transcoder functionality within a single call. A transcoder takes the stream of one codec and transcodes (converts) it from one compression type to another compression type. For example, it could take a stream from a G.711 codec and transcode (convert) it in real time to a G.729 stream. In addition, a transcoder provides MTP capabilities and may be used to enable supplementary services for H.323 endpoints when required.

For each media termination point device and each transcoder that is registered with Cisco Unified Communications Manager, Cisco Unified Communications Manager creates a media termination point control
process. This media termination point control process registers with the device manager when it initializes. The device manager advertises the availability of the media termination point control processes throughout the cluster.

**Annunciator Control**

An annunciator enables Cisco Unified Communications Manager to play prerecorded announcements (.wav files) and tones to Cisco Unified IP Phones, gateways, and other configurable devices. The annunciator, which works with Cisco Unified Communications Manager Multilevel Precedence and Preemption, enables Cisco Unified Communications Manager to alert callers as to why the call fails. Annunciator can also play tones for some transferred calls and some conferences.

For each annunciator device that is registered with Cisco Unified Communications Manager, Cisco Unified Communications Manager creates an annunciator control process. This annunciator control process registers with the device manager when it initializes. The device manager advertises the availability of the annunciator control process throughout the cluster.

**Unicast Bridge Control**

A unicast bridge (CFB), more commonly known as a conference bridge, provides the capability to mix a set of incoming unicast streams into a set of composite output streams. Unicast bridge provides resources to implement ad hoc and meet-me conferencing in the Cisco Unified Communications Manager.

For each unicast bridge device that is registered with Cisco Unified Communications Manager, Cisco Unified Communications Manager creates a unicast control process. This unicast control process registers with the device manager when it initializes. The device manager advertises the availability of unicast stream resources throughout the cluster.

**Music On Hold Control**

Music on hold (MOH) provides the capability to redirect a party on hold to an audio server. For each music on hold server device that is registered with Cisco Unified Communications Manager, Cisco Unified Communications Manager creates a music on hold control process. This music on hold control process registers with the device manager when it initializes. The device manager advertises the availability of music on hold resources throughout the cluster. Music on hold supports both unicast and multicast audio sources.

**Trusted relay point**

The Cisco Unified Communications system can be deployed in a network virtualization environment. Cisco Unified Communications Manager enables the insertion of trusted relay points (TRPs). The insertion of TRPs into the media path constitutes a first step toward VoIP deployment within a virtual network.

The underlying network infrastructure comprises one of the key shared assets in an overall network design. A number of customer use cases require support for network infrastructure virtualization, such as the following examples:

- Guest internet access
- Partner access
- Departmental or divisional separation
- Subsidiaries/mergers and acquisitions
- Application segregation (data/voice)
All these applications include a requirement to maintain traffic separation on the network device as well as between network devices.

Traffic separation translates into concepts such as Virtual Routing and Forwarding (VRF). VRF allows multiple instances of a routing table to co-exist within the same router at the same time. In a virtualized network, these different routing domains, or VRFs, typically cannot communicate directly without transiting through the data center. This situation challenges applications such as Cisco Unified Communications, where devices in the data VRF domain, such as software endpoints running on PCs, need to communicate directly with hard phones in the voice VRF domain without hairpinning media in the data center and without directly exposing the voice and data VRFs to each other.

**Inter-VRF communication**

To solve the communication problem between PC-based softphones located in the data VRF domain and the hard phones located in the voice VRF domain without hairpinning media in the data center and without directly exposing the voice and data VRFs to each other, the system can insert a trusted relay point (TRP) in the media path between the softphone and hard phone, so both phones send/receive media to the TRP, and the TRP relays the media from one phone to another phone. The system allows only media that passes through the TRP between voice and data VRF domains.

*Figure 24: Inter-VRF Communication With TRPs*

**Media firewall traversal**

A firewall currently must inspect the signaling of the call setup to open pinholes for Real-time Transfer Protocol (RTP) streams. Many deployments of firewalls exist in such a way that a customer can design their network, so only media go through the firewall, but not the signaling.

If a firewall has media termination point (MTP)/trusted relay point (TRP) functionality, Cisco Unified Communications Manager can insert the MTP/TRP in the media path, so the signaling does not have to go through the firewall for the RTP streams to traverse the firewall and at the same time be inspected at the firewall. The firewall receives signaling from Cisco Unified Communications Manager, which informs about the RTP traffic.

The firewall can allow this traffic because of the messaging from Cisco Unified Communications Manager, but the firewall does not have to allow this traffic if the firewall is so configured. If the local configuration
on the firewall prevents these RTP streams, calls never start only to be dropped at the firewall interface. After a firewall receives indication that the stream comes from phones, that firewall can still inspect all the RTP streams to ensure that everything appears as it should between the two devices that are communicating and that someone is not trying to attack the phone system.

**Figure 25: Media Firewall Traversal**

---

**Quality-of-Service enforcement**

In a Cisco voice network, the switch detects Cisco Unified IP Phones that use Cisco Discovery Protocol (CDP), and the switch trusts the Differentiated Services Code Point (DSCP) marking of packets that the Cisco Unified IP Phones send. Because CDP is not secure and can easily be replicated from a PC, the switch generally does not trust the traffic that is coming from a PC. Because it is almost impossible to ensure that only Cisco Unified Communications Manager-authorized traffic will get marked with DSCP, the packets that come from a PC get re-marked to best effort.

To resolve this problem, Cisco Unified Communications Manager inserts a trusted relay point (TRP) in front of the softphone that runs on the PC, and the media stream from the endpoint can be forced to flow through the TRP. The TRP re-marks the DSCP according to instructions from Cisco Unified Communications Manager. The switch honors and trusts media packets that are sent from the TRP.

**Figure 26: QoS Enforcement by TRPs**

---

**Trusted relay point service parameter**

Cisco Unified Communications Manager uses the following service parameter with trusted relay points:

- Fail Call If Trusted Relay Point Allocation Fails

This service parameter, which is found in the Clusterwide Parameters (System - General) section, determines whether a call that requires a Trusted Relay Point (TRP) is allowed to proceed if no TRP resource is available. Valid values specify True (the call fails if no TRP resource is available) or False (the call proceeds regardless even if a TRP resource is not available).
The administrator should choose the best value for a system based on how the system uses TRPs. If a TRP is used for Quality of Service (QoS) enforcement, Cisco Unified Communications Manager can complete the call if a TRP resource is unavailable, but the call will not have the correct Differentiated Services Code Point (DSCP) marking.

**TRP insertion in Cisco Unified Communications Manager**

From the Cisco Unified Communications Manager point of view, the trusted relay point (TRP) always gets placed closest to the endpoint device that requires it. The high-level requirements for TRP insertion follow:

- The administrator configures the Use Trusted Relay Point check box in the Common Device Configuration window. The administrator configures the Use Trusted Relay Point drop-down list with On/Off/Default options in the configuration windows of all devices where media terminate, so Cisco Unified Communications Manager knows when to insert a TRP.

- The administrator configures the Trusted Relay Point check box in the Media Termination Point Configuration and Transcoder Configuration windows. If the administrator checks this check box when configuring a particular device, Cisco Unified Communications Manager knows that it can use the device as a TRP. The administrator must ensure that a device that is configured as a TRP in Cisco Unified Communications Manager has the appropriate network connectivity and configuration between the TRP and any endpoints that are involved in the call. If the TRP is invoked but does not have the needed connectivity, an audio or video call will not succeed.

- The service parameter, Fail Call If Trusted Relay Point Allocation Fails, applies. See the Trusted relay point service parameter, on page 250 for details.

- Cisco Unified Communications Manager must insert a TRP for the endpoint if the Use Trusted Relay Point check box is checked for either the endpoint or the device pool that is associated with the device. The call may fail if Cisco Unified Communications Manager fails to allocate a TRP while the Fail Call If Trusted Relay Point Allocation Fails service parameter is set to True.

- If both the Media Termination Point Required check box and the Use Trusted Relay Point check box are checked for the endpoint, Cisco Unified Communications Manager should allocate an MTP that is also a TRP. If the administrator fails to allocate such an MTP/TRP, the following table shows the call status, which the values of the Fail Call If Trusted Relay Point Allocation Fails service parameter and the Fail Call if MTP Allocation Fails service parameter also affect.

<table>
<thead>
<tr>
<th>Fail Call If TRP Allocation Fails</th>
<th>Fail Call If MTP Allocation Fails</th>
<th>Fail Call?</th>
</tr>
</thead>
<tbody>
<tr>
<td>True</td>
<td>True</td>
<td>Yes</td>
</tr>
<tr>
<td>True</td>
<td>False</td>
<td>Yes</td>
</tr>
<tr>
<td>False</td>
<td>True</td>
<td>Yes, if MTP is required for H.323 endpoint. No, if MTP is required for SIP endpoint.</td>
</tr>
<tr>
<td>False</td>
<td>False</td>
<td>No</td>
</tr>
</tbody>
</table>
• If RSVP is enabled for the call, Cisco Unified Communications Manager should first try to allocate an RSVP Agent that is also labeled as TRP. Otherwise, another TRP device gets inserted between the RSVP Agent and the endpoint.

• If a transcoder is needed for the call and needs to be allocated on the same side as the endpoint that needs TRP, Cisco Unified Communications Manager should first try to allocate a transcoder that is also labeled as TRP. Otherwise, another TRP device gets inserted between the transcoder and the endpoint.

• Assuming that both the Fail Call If Trusted Relay Point Allocation Fails service parameter and the Fail Call If MTP Allocation Fails service parameter are set to False, the following table shows the call behavior in relationship to the MTP that is required and Use Trusted Relay Point settings and the resource allocation status.

<table>
<thead>
<tr>
<th>MTP Required</th>
<th>Use TRP</th>
<th>Resource Allocation Status</th>
<th>Call Behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>Y</td>
<td>Y</td>
<td>TRP allocated</td>
<td>Audio call only because no pass-through support exists.</td>
</tr>
<tr>
<td>Y</td>
<td>Y or N</td>
<td>MTP only</td>
<td>Audio call only. No TRP support.</td>
</tr>
<tr>
<td>Y</td>
<td>Y or N</td>
<td>None allocated</td>
<td>If MTP required is checked for H.323 endpoint, supplementary services will be disabled.</td>
</tr>
<tr>
<td>N</td>
<td>Y</td>
<td>TRP allocated</td>
<td>Audio or video call depends on endpoint capabilities, and call admission control (CAC). Supplementary services still work.</td>
</tr>
<tr>
<td>N</td>
<td>Y</td>
<td>None allocated</td>
<td>Audio or video call. Supplementary services still work, but no TRP support exists.</td>
</tr>
</tbody>
</table>

• In most instances, TRP is allocated after users answer the call, so if a call fails due to failure to allocate the TRP, users may receive fast-busy tone after answering the call. (The SIP outbound leg with MTP required, or H.323 outbound faststart, represents an exception.)

**Media resource groups**

Cisco Unified Communications Manager media resource groups and media resource group lists provide a way to manage resources. Use these resources for conferencing, transcoding, media termination, and music on hold (MOH).

Media resource groups define logical groupings of media servers. You can associate a media resource group with a geographical location or a site as desired. You can also form media resource groups to control the usage of servers or the type of service (unicast or multicast) that is desired.

After media resources are configured, if no media resource groups are defined, all media resources belong to the default group, and, as such, all media resources are available to all Cisco Unified Communications Managers within a given cluster.
Deactivating the Cisco IP Voice Media Streaming Application deletes associated devices (Annunciator, Conference Bridge, Music-on-Hold, and Media Termination Point) from media resource groups. If the deletion results in an empty media resource group, you cannot deactivate the service; in this case, you must delete the media resource group before deactivating the service.

The following rules govern selection of a resource from a media resource group in a media resource group list:

- Search the first media resource group in a media resource group list to find the requested resource. If located, return the resource ID.
- If the requested resource is not found, search the next media resource group in the media resource group list. Return the resource ID if a match is found.
- If no resource of the requested type is available in any media resource group in a media resource group list, the resource manager attempts to use the resource in the default group.

**Example**

The default media resource group for a Cisco Unified Communications Manager comprises the following media resources: MOH1, MTP1, XCODE1, XCODE2, XCODE3. For calls that require a transcoder, this Cisco Unified Communications Manager distributes the load evenly among the transcoders in its default media resource group. The following allocation order occurs for incoming calls that require transcoders:

<table>
<thead>
<tr>
<th>Call</th>
<th>Resource</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>XCODE1</td>
</tr>
<tr>
<td>2</td>
<td>XCODE2</td>
</tr>
<tr>
<td>3</td>
<td>XCODE3</td>
</tr>
<tr>
<td>4</td>
<td>XCODE1</td>
</tr>
<tr>
<td>5</td>
<td>XCODE2</td>
</tr>
<tr>
<td>6</td>
<td>XCODE3</td>
</tr>
<tr>
<td>7</td>
<td>XCODE1</td>
</tr>
</tbody>
</table>

**Media resource group lists**

Media resource group lists specify a list of prioritized media resource groups. An application can select required media resources from among the available resources according to the priority order that is defined in the media resource group list. Media resource group lists, which are associated with devices, provide media resource group redundancy.

The following rules govern selection of media resource group lists:

- A media resource group list, which is configured in the Media Resource Group List Configuration window, gets assigned to either a device or to a device pool.
- Call processing uses a media resource group list in the device level if the media resource group list is selected. If a resource is not found, call processing may retrieve it from the default allocation.
- Call processing uses media resource group list in the device pool only if no media resource group list is selected in the device level. If a resource is not found, call processing may retrieve it from the default allocation.
Example of Using Media Resource Group List to Group Resources by Type

Assign all resources to three media resource groups as listed:

- **SoftwareGroup** media resource group: MTP1, MTP2, SW-CONF1, SWCONF2
- **HardwareGroup** media resource group: XCODE1, XCODE2, HW-CONF1, HW-CONF2
- **MusicGroup** media resource group: MOH1, MOH2

Create a media resource group list called RESOURCE_LIST and assign the media resource groups in this order: SoftwareGroup, HardwareGroup, MusicGroup.

Result: With this arrangement, when a conference is needed, Cisco Unified Communications Manager allocates the software conference resource first; the hardware conference does not get used until all software conference resources are exhausted.

Example of Using Media Resource Group List to Group Resources by Location

Assign resources to four media resource groups as listed:

- **DallasSoftware**: MTP1, MOH1, SW-CONF1
- **SanJoseSoftware**: MTP2, MOH2, SW-CONF2
- **DallasHardware**: XCODE1, HW-CONF1
- **SanJoseHardware**: XCODE2, HW-CONF2

CM1 and CM2 designate Cisco Unified Communications Managers.

Create a DALLAS_LIST media resource group list and assign media resource groups in this order: DallasSoftware, DallasHardware, SanJoseSoftware, SanJoseHardware.

Create a SANJOSE_LIST media resource group list and assign media resource groups in this order: SanJoseSoftware, SanJoseHardware, DallasSoftware, DallasHardware.

Assign a phone in Dallas CM1 to use DALLAS_LIST and a phone in San Jose CM2 to use SANJOSE_LIST.

Result: With this arrangement, phones in CM1 use the DALLAS_LIST resources before using the SANJOSE_LIST resources.

Example of Using Media Resource Group List to Restrict Access to Conference Resources

Assign all resources to four groups as listed, leaving no resources in the default group:

- **MtpGroup**: MTP1, MTP2
- **ConfGroup**: SW-CONF1, SW-CONF2, HW-CONF1, HW-CONF2
- **MusicGroup**: MOH1, MOH2
- **XcodeGroup**: XCODE1, XCODE2

Create a media resource group list that is called NO_CONF_LIST and assign media resource groups in this order: MtpGroup, XcodeGroup, MusicGroup.

In the device configuration, assign the NO_CONF_LIST as the device media resource group list.

Result: The device cannot use conference resources. This means that only media termination point, transcoder, annunciator, and music resources are available to the device.
Related Topics

Device pools, on page 45

Dependency records

To find out which media resource group lists are associated with the media resource groups, click the Dependency Records link that displays in the Cisco Unified Communications Manager Administration Media Resource Group Configuration window. To find out more information about the media resource group list, click the record type, and the Dependency Records Details window displays.

To find out which phones or trunks are associated with media resource group lists, click the Dependency Records link that displays in the Cisco Unified Communications Manager Administration Media Resource Group List Configuration window.

If the dependency records are not enabled for the system, the dependency records summary window displays a message.
Dependency records
Annunciator

This chapter provides information about an annunciator, which is an SCCP device that uses the Cisco IP Voice Media Streaming Application service, enables Cisco Unified Communications Manager to play prerecorded announcements (.wav files) and tones to Cisco Unified IP Phones, gateways, and other configurable devices. The annunciator, which works with Cisco Unified Communications Manager Multilevel Precedence and Preemption, enables Cisco Unified Communications Manager to alert callers as to why the call fails. Annunciator can also play tones for some transferred calls and some conferences.

Configure annunciator, page 257
Annunciators overview, page 258
Secured annunciator through SRTP, page 259
Plan annunciator configuration, page 261
Annunciator system requirements and limitations, page 262
Supported tones and announcements, page 263
Dependency records, page 264
Annunciator performance monitoring and troubleshooting, page 264

Configure announciator

An annunciator, an SCCP device that uses the Cisco IP Voice Media Streaming Application service, enables Cisco Unified Communications Manager to play prerecorded announcements (.wav files) and tones to Cisco Unified IP Phones, gateways, and other configurable devices. The annunciator, which works with Cisco Unified Communications Manager Multilevel Precedence and Preemption, enables Cisco Unified Communications Manager to alert callers as to why the call fails. Annunciator can also play tones for some transferred calls and some conferences.

Configure an annunciator as follows.
Procedure

**Step 1** Determine the number of annunciator streams that are needed and the number of annunciators that are needed to provide these streams.

**Step 2** Verify that you have activated the Cisco IP Voice Media Streaming Application service on the server where you want the annunciator to exist.

**Step 3** Perform additional annunciator configuration tasks if you want to change the default settings.

**Step 4** Add the new annunciators to the appropriate media resource groups and media resource lists.

**Step 5** Reset or restart the individual annunciator or all devices that belong to the media resource group/list.

Related Topics

- Media resource management, on page 245

Annunciators overview

In conjunction with Cisco Unified Communications Manager, the annunciator device provides multiple, one-way, RTP stream connections to devices, such as Cisco Unified IP Phones and gateways.

To automatically add an annunciator to the Cisco Unified Communications Manager database, you must activate the Cisco IP Voice Media Streaming Application service on the server.

---

**Note**

When you add a server, the annunciator device automatically gets added for the new server. It will remain inactive until the Cisco IP Voice Media Streaming Application service is activated for the new server.

Cisco Unified Communications Manager uses SCCP messages to establish a RTP stream connection between the annunciator and the device. The annunciator plays the announcement or tone to support the following conditions:

- Announcement-Devices configured for Cisco Multilevel Precedence and Preemption
- Barge tone-Before a participant joins an ad hoc conference
- Ring back tone-When you transfer a call over the PSTN through an IOS gateway
  Annunciator plays the tone because the gateway cannot play the tone when the call is active.
- Ring back tone-When you transfer calls over an H.323 intercluster trunk
- Ring back tone-When you transfer calls to the SIP client from a phone that is running SCCP

---

**Tip**

For specific information about supported announcements and tones, see the Supported tones and announcements, on page 263.

Before the announcement/tone plays, the annunciator reads the following information from the annunciator.xml file in the Cisco Unified Communications Manager database:
• The TypeAnnouncements database table, which is read into memory cache to identify each announcement or tone that the annunciator supports.

• The user locale identifier for the phone, which is added to the database if you install the Cisco Unified Communications Manager Locale Installer.

• The network locale identifier for the phone or gateway, which is added to the database if you install the Cisco Unified Communications Manager Locale Installer.

• The device settings

• The user-configured service parameters

Secured annunciator through SRTP

Cisco Unified Communications Manager 8.6(1) and later enhances the Cisco IP Voice Media Streaming application service to support Secure Real-Time Protocol (SRTP); therefore, when the Cisco Unified Communications Manager is enabled for security, the annunciator registers with the Cisco Unified Communications Manager as an SRTP capable device. If the receiving device is also SRTP capable, the announcements are encrypted before streaming to the receiving device.

In a secure mode, the Cisco Unified Communications Manager Administration device page for Annunciator displays a Device is trusted message with a check box, indicating that it is a trusted device.

When the Cisco Unified Communications Manager is configured in a secure deployment environment (the Cluster Security Mode enterprise parameter is set to mixed mode), Cisco Unified IP Phones, voice gateways, and other secure capable endpoints are set to encrypted mode. The media streaming between the devices is done through SRTP. When calls are secure, a locked icon displays on the Cisco Unified IP Phone, indicating that the call is protected for both signaling and the media.

When the secured annunciator plays an announcement, the Cisco Unified IP Phone that receives the announcement displays a locked icon. When the secured annunciator plays a ringback tone, such as in the case of a caller performing a blind transfer over a SIP or H.323 intercluster trunk, the Cisco Unified IP Phone to be transferred displays the locked icon while the annunciator plays the ringback tone to it.

When Cisco Unified Communications Manager interrupts the media of an encrypted call, such as when call features are activated, the locked icon is removed from the Cisco Unified IP Phone. The icon is restored when the phone reconnects with the encrypted media. The duration of the media interruption and restoration is short when encrypted annunciator is activated.

Security enabled for annunciator

Annunciator devices are automatically enabled for security when the enterprise parameter Cluster Security Mode is set to 1 (mixed mode).

Related Topics

Server configuration, on page 30
Secured and non-secured announcements

The following examples provide scenarios that describe how the locked icon displays when secured and non-secured announcements are inserted to the calls.

**Encrypted announcement for a precedence call**

The following example describes an encrypted announcement for a precedence call.

1. User 4000 dials 99 3000 to reach user 3000. The Cisco Unified Communications Manager configured a translation pattern of 99.XXXX to enable users to dial a prefix of 99 to initiate an MLPP Flash Override call.

2. Cisco Unified Communications Manager dials user 3000 and user 3000 answers the call. Prior to answering the call, user 3000 was on an MLPP Flash call. When user 3000 answered the call, the busy trigger limit was reached.

3. The media between user 4000 and user 3000 is set up with SRTP; therefore, the secure locked icon displays on the phones for user 4000 and 3000.

4. User 2000 dials 88 3000 to call user 3000. Cisco Unified Communications Manager configured a translation pattern of 88.XXXX to enable users to dial a prefix of 88 to initiate an MLPP Flash Override call.

5. Because user 3000 has reached the call busy trigger limit and all of the calls have equal (Flash) or higher (Flash Override) precedence levels, Cisco Unified Communications Manager rejects the call from user 2000 with an MLPP-BPA announcement. Because both the user device and the announcement are encrypted, the announcement plays by using SRTP. The locked icon displays on the IP phone of user 2000.

**Unencrypted announcement for a precedence call**

The following example describes an unencrypted announcement for a precedence call. In this example, the device for user 2000 is unencrypted (non-secure). Therefore, the MLPP-BPA announcements is played to the user by using RTP and no secure locked icon displays on the IP phone.

1. User 3000 dials 77 2000 to reach user 2000. Cisco Unified Communications Manager configured a translation pattern of 77.XXXX to enable users to dial a prefix of 77 to initiate an MLPP Immediate call.

2. Cisco Unified Communications Manager dials user 2000 and user 2000 answers the call. Prior to answering the call, user 2000 was on an MLPP Priority call. When user 2000 answered the call, the busy trigger limit was reached.

3. The media between user 3000 and user 2000 is set up with SRTP; therefore, the locked icon displays on the phones for user 3000 and 2000.

4. User 1000 dials 66 2000 to call user 2000. Cisco Unified Communications Manager configured a translation pattern of 66.XXXX to enable users to dial the prefix 66 to initiate an MLPP Flash call.

5. Because user 2000 has reached the call busy trigger limit and all of the calls have equal (Priority) or higher (Immediate) precedence levels, Cisco Unified Communications Manager rejects the call from user 1000 with an MLPP-BPA announcement. Because user 2000 is using an unencrypted (non-secure) device, the announcement plays by using RTP and no locked icon displays on the IP phone.

**Unencrypted announcement for a precedence call when security mode is overridden**

The following example describes an unencrypted announcement for a precedence call when the security mode of the Annunciator is overridden. The Make Annunciator Non-secure when Cluster Security is Mixed service

Cisco Unified Communications Manager System Guide, Release 9.0(1)
parameter, an advanced service parameter for the Cisco Unified IP Voice Media Streaming App, can override the security mode of the Announcer. If this parameter is set to True, the unencrypted announcement is played to the caller even though the calling device is SRTP capable.

1. User 3000 dials 77 2000 to reach user 2000. Cisco Unified Communications Manager configured a translation pattern of 77.XXXX to enable users to dial a prefix of 77 to initiate an MLPP Immediate call.

2. Cisco Unified Communications Manager dials user 2000 and user 2000 answers the call. Prior to answering the call, user 2000 was on an MLPP Priority call. When user 2000 answered the call, the busy trigger limit was reached.

3. The media between user 3000 and user 2000 is set up with SRTP; therefore, the locked icon displays on the phones for user 3000 and user 2000.

4. User 1000 dials 66 2000 to call user 2000. Cisco Unified Communications Manager configured a translation pattern of 66.XXXX to enable users to dial the prefix 66 to initiate an MLPP Flash call.

5. Because user 2000 has reached the call busy trigger limit and all of the calls have equal (Priority) or higher (Immediate) precedence levels, Cisco Unified Communications Manager rejects the call from user 1000 with an MLPP-BPA announcement. The Annunciator is unencrypted (non-secure) because the advanced service parameter was used to override the security mode of the cluster system. The announcement plays by using RTP even though the device for user 1000 is SRTP capable. No locked icon displays on the IP phone of user 1000.

**Encrypted announcement for a call to a number that does not exist**

The following example describes an encrypted announcement for a call to a number that does not exist. When you dial a number that does not exist in the Cisco Unified Communications Manager database, you receive a VCA announcement. If your IP phone is SRTP capable, the announcement is encrypted.

1. User 2000 dials the number 9999. This number does not exist in the Cisco Unified Communications Manager database; therefore, there is no routing path for the pattern.

2. Cisco Unified Communications Manager plays the VCA announcement to user 2000. Because both the Annunciator and the IP phone for user 2000 are capable of SRTP, the VCA announcement is encrypted and the locked icon displays on the phone.

**Plan annunciator configuration**

Consider the following information before you plan your annunciator configuration. Use this information in conjunction with the Annunciator system requirements and limitations, on page 262.

- For a single annunciator, Cisco Unified Communications Manager sets the default to 48 simultaneous streams, as indicated in the annunciator service parameter for streaming values.

---

**Caution**

Cisco recommends that you do not exceed 48 annunciator streams on a coresident server where the Cisco Unified Communications Manager and Cisco IP Voice Media Streaming Application services run.

- You can change the default to best suit your network. For example, a 100-MB Network/NIC card can support 48 annunciator streams, while a 10-MB NIC card supports up to 24 annunciator streams. The
exact number of annunciator streams that are available depends on the factors, such as the speed of the processor and network loading.

- If the annunciator runs on a standalone server where the Cisco Unified Communications Manager service does not run, the annunciator can support up to 255 simultaneous announcement streams.
- If the standalone server has dual CPU and a high-performance disk system, the annunciator can support up to 400 simultaneous announcement streams.

Consider the following formula to determine the approximate number of annunciators that you need for your system. This formula assumes that the server can handle the default number of streams (48); you can substitute the default number for the number of streams that your server supports.

\[
n \div \text{number of annunciator devices that your server supports}
\]

where:

- \(n\) represents the number of devices that require annunciator support

Tip

If a remainder exists in the quotient, consider adding another server to support an additional annunciator device. To perform this task, activate the Cisco IP Voice Media Streaming Application service on another server and update the configuration of the device, if you do not want to use the default settings.

Annunciator system requirements and limitations

The following system requirements and limitations apply to annunciator devices:

- For one annunciator device, activate only one Cisco IP Voice Media Streaming Application service in the cluster. To configure additional annunciators, you must activate the Cisco IP Voice Media Streaming Application service on additional Cisco Media Convergence Servers or Cisco-approved, third-party servers where Cisco Unified Communications Manager is installed in the cluster.

Caution

Cisco strongly recommends that you do not activate the Cisco IP Voice Media Streaming Application service on a Cisco Unified Communications Manager with a high call-processing load.

- Each annunciator belongs to a device pool.
- Each annunciator can support G.711 a-law, G.711 mu-law, wideband, and G.729 codec formats.
- For information on the number of streams that are available for use, see the Plan announciator configuration, on page 261.
- To manage the media resources, you can add the annunciator to a Media Resource Group, and likewise, a Media Resource List.
- When you update the annunciator, the changes automatically occur when the annunciator becomes idle, when no active announcements are played.
- Cisco Unified Communications Manager provides annunciator resource support to a conference bridge under the following circumstances:
If the media resource group list that contains the annunciator is assigned to the device pool where the conference bridge exists.

If the annunciator is configured as the default media resource, which makes it available to all devices in the cluster.

Cisco Unified Communications Manager does not provide annunciator resource support for a conference bridge if the media resource group list is assigned directly to the device that controls the conference.

**Supported tones and announcements**

Cisco Unified Communications Manager automatically provides a set of recorded annunciator announcements when you activate the Cisco IP Media Streaming Application service. No configuration exists to customize these announcements or to add new announcements.

Annunciator announcements, which comprise one or two wav files, support localization if you have installed the Cisco Unified Communications Manager Locale Installer and configured the locale settings for the Cisco Unified IP Phone or, if applicable, the device pool. Each announcement plays in its entirety.

Cisco Unified Communications Manager supports only one announcement per conference. During a conference, if the system requests a new announcement while another announcement currently plays, the new announcement preempts the other announcement.

Annunciator supports the announcements in Table 21-2.

**Table 24: Announcements**

<table>
<thead>
<tr>
<th>Condition</th>
<th>Announcement</th>
</tr>
</thead>
<tbody>
<tr>
<td>An equal or higher precedence call is in progress.</td>
<td>Equal or higher precedence calls have prevented the completion of your call. Please hang up and try again. This is a recording.</td>
</tr>
<tr>
<td>A precedence access limitation exists.</td>
<td>Precedence access limitation has prevented the completion of your call. Please hang up and try again. This is a recording.</td>
</tr>
<tr>
<td>Someone attempted an unauthorized precedence level.</td>
<td>The precedence used is not authorized for your line. Please use an authorized precedence or ask your operator for assistance. This is a recording.</td>
</tr>
<tr>
<td>The call appears busy, or the administrator did not configure the directory number for call waiting or preemption.</td>
<td>The number you have dialed is busy and not equipped for call waiting or preemption. Please hang up and try again. This is a recording.</td>
</tr>
<tr>
<td>The system cannot complete the call.</td>
<td>Your call cannot be completed as dialed. Please consult your directory and call again or ask your operator for assistance. This is a recording.</td>
</tr>
</tbody>
</table>
Announcement
Condition
A service interruption occurred.

Announcement
A service disruption has prevented the completion of your call. In case of emergency call your operator. This is a recording.

Annunciator supports the following tones:

• Busy tone
• Alerting/Ring back tone
• Conference barge-in tone

Dependency records
To find which media resource groups include an annunciator device, choose Dependency Records from the Related Links drop-down list box and click Go. The Dependency Records Summary window displays information about media resource groups that use the annunciator device. To find out more information about the media resource group, click the media resource group, and the Dependency Records Details window displays. If the dependency records are not enabled for the system, the dependency records summary window displays a message.

Annunciator performance monitoring and troubleshooting
Performance Monitor counters for annunciator allow you to monitor the number of streams that are used, the streams that are currently active, the total number of streams that are available for use, the number of failed annunciator streams, the current connections to the Cisco Unified Communications Manager, and the total number of times a disconnection occurred from the Cisco Unified Communications Manager. When an annunciator stream is allocated or de-allocated, the performance monitor counter updates the statistic. For more information about performance monitor counters, see the Cisco Unified Serviceability Administration Guide.

Cisco Unified Communications Manager writes all errors for the annunciator to the Event Viewer. In Cisco Unified Communications Manager Serviceability, you can set traces for the Cisco IP Voice Media Streaming Application service; to troubleshoot most issues, you must choose the Significant or Detailed option for the service, not the Error option. Reset trace level to the Error option after you troubleshoot the issue.

Cisco Unified Communications Manager generates registration and connection alarms for annunciator in Cisco Unified Serviceability. For more information on alarms, see the Cisco Unified Serviceability Administration Guide.

If you need technical assistance, use the Real-Time Monitoring Tool to retrieve the cms/sdi trace log files before you contact your Cisco Partner or the Cisco Technical Assistance Center (TAC).
Conference bridges

This chapter provides information about Conference Bridges for Cisco Unified Communications Manager which designates a software or hardware application that is designed to allow both ad hoc and meet-me voice conferencing. Additional conference bridge types support other types of conferences, including video conferences. Each conference bridge can host several simultaneous, multiparty conferences.

- Configure conference bridge, page 265
- Conference devices overview, page 266
- Conference types, page 273
- Conferences and the party entrance tone, page 280
- Intelligent bridge selection, page 281
- Dependency records, page 284
- Conference bridge performance monitoring and troubleshooting, page 285

Configure conference bridge

Conference Bridge for Cisco Unified Communications Manager designates a software or hardware application that is designed to allow both ad hoc and meet-me voice conferencing. Additional conference bridge types support other types of conferences, including video conferences. Each conference bridge can host several simultaneous, multiparty conferences.

Conference Bridge includes the following features:

- Creating a conference call
- Adding new participants to an existing conference call
- Ending a conference call
- Dropping conference participants
- Canceling a conference call
- Parking a conference call
- Transferring a conference call
The checklist to configure conference bridge is as follows.

**Procedure**

- **Step 1** Configure the hardware or software conference bridge(s).
- **Step 2** Configure the Meet-Me Number/Pattern.
- **Step 3** Add a Conference button for ad hoc or Meet Me Conference button for the meet-me conference to the phone templates, if needed. You only need to do this for Cisco Unified IP Phones 12 SP, 12 SP+, and 30 VIP.
- **Step 4** If users will use the Join, ConfList, and RmLstC softkeys, modify either the Standard Feature or Standard User softkey template and assign the modified softkey template to the user device.
- **Step 5** Configure the ad hoc conference settings.
- **Step 6** Notify users that the Conference Bridge feature is available. If applicable, notify users of the meet-me conference number range.

See the phone documentation for instructions on how users access conference bridge features on their Cisco Unified IP Phone.

---

**Conference devices overview**

Cisco Unified Communications Manager supports multiple conference devices to distribute the load of mixing audio between the endpoints involved in a conference. A component of Cisco Unified Communications Manager called Media Resource Manager (MRM) locates and assigns resources. The MRM resides on every Cisco Unified Communications Manager server and communicates with MRMs on other Cisco Unified Communications Manager servers.

Cisco Unified Communications Manager supports hardware and software conference devices; both hardware and software conference bridges can be active at the same time.

For conferencing, you must determine the total number of concurrent users (or audio streams) that are required at any given time. (An audio stream is a two-way audio path in a conference that supports one stream for each endpoint/participant.) Then, if you plan to use a software conference device, you create and configure the device to support the calculated number of streams (see the Software conference devices, on page 267 for information about calculating number of streams). You cannot configure the number of streams for hardware conference bridges. One large conference, or several small conferences, can use these audio streams.

**Caution**

Although a single software conference device can run on the same server as the Cisco Unified CallManager service, Cisco strongly recommends against this configuration. Running a conference device on the same server as the Cisco CallManager service may adversely affect performance on the Cisco Unified Communications Manager.

---

**Router-based conference capability**

The Cisco 1700, Cisco 2600, Cisco 2600XM, Cisco 2800, Cisco 3600, Cisco 3700, and Cisco 3800 series voice gateway routers provide conferencing capabilities for Cisco Unified Communications Manager. These routers provide conferencing with two features:
Cisco Conferencing and Transcoding for Voice Gateway Routers by using the NM-HDV or NM-HDV-FARM network modules. This feature supports up to six parties in a conference. (Choose the Cisco IOS Conference Bridge from the Conference Bridge Configuration window in Cisco Unified Communications Manager Administration to support this feature.)

Cisco Enhanced Conferencing and Transcoding for Voice Gateway Routers by using the Cisco Packet Voice/Fax Digital Signal Processor Modules (PVDM2) on the Cisco 2800 and 3800 series voice gateway routers or using the NM-HD-xx or NM-HDV2 network modules. This feature supports eight parties in a conference. (If you are using a version of Cisco IOS that allows you to specify the Communications Manager version number, ensure this version matches that of your Communications Manager and choose the Cisco IOS Enhanced Conference Bridge from the Conference Bridge Configuration window in Cisco Unified Communications Manager Administration to support this feature. If you are using a Cisco IOS version that does not allow you to specify the Communications Manager version number, choose the Cisco IOS Conference Bridge instead.)

For more information about these conferencing routers, see the IOS router documentation provided with your router.

Router-enabled conferencing provides the ability to support voice conferences in hardware. Digital Signal Processors (DSPs) convert multiple Voice over IP Media Streams into TDM streams that are mixed into a single conference call stream. The DSPs support both meet-me and ad hoc conferences by Cisco Unified Communications Manager.

The Cisco routers that support conferencing have the following codecs:

- G.711 a/u-law
- G.729, G.729a, G.729b, G.729ab
- GSM FR, GSM EFR (only supports Cisco Enhanced Conferencing and Transcoding for Voice Gateway Routers feature)

Software conference devices

For software conference devices, you can adjust the number of streams because software conference devices support a variable number of audio streams. You can configure a software conference device and choose the number of full-duplex audio streams that the device supports. To calculate the total number of conferences that a device supports, divide the number of audio streams by three (the minimum number of participants in a conference). The maximum number of audio streams equals 128. For more information on software conference devices, see the Conference bridge types in Cisco Unified Communications Manager administration, on page 268.

Video conference devices

The Cisco Video Conference Bridge, a dual multimedia bridge, provides video conferencing. Cisco Unified Communications Manager controls this conference bridge type upon appropriate configuration. The Cisco Video Conference Bridge provides audio and video conferencing functions for Cisco IP video phones, H.323 endpoints, and audio-only Cisco Unified IP Phones. Administrators can partition the resources of the Cisco video conference bridge between the video telephony network and the H.323/SIP network. The Cisco Video Conference Bridge supports the H.261, H.263, and H.264 codecs for video.

To configure this type of conference device, the user chooses the Cisco Video Conference Bridge (IPVC-35xx) conference bridge type in Cisco Unified Communications Manager Administration.
To ensure that only a video conference bridge gets used when a user wants to hold a video conference, add the video conference bridge to a media resource group. Add the media resource group to a media resource group list and assign the media resource group list to the device or device pool that will use the video conference bridge. See Conference bridge types in Cisco Unified Communications Manager administration, on page 268 for details.

**Cisco conference devices (WS-SVC-CMM)**

Applications can control a Cisco Unified Communications Manager Conference Bridge (WS-SVC-CMM). For more information on Cisco Conference Devices (WS-SVC-CMM), see the Conference bridge types in Cisco Unified Communications Manager administration, on page 268.

To configure this type of conference device, the user chooses the Cisco Conference Bridge (WS-SVC-CMM) conference bridge type in Cisco Unified Communications Manager Administration

**MTP WS-X6608 DSP service card**

Because hardware conference devices are fixed at 32 full-duplex streams per WS-X6608 port, hardware conference devices support 32 divided by three (32/3), or 10, conferences. Users cannot change this value.

---

**Caution**

Full-duplex streams per WS-X6608 port cannot exceed the maximum limit of 32.

---

**Annunciator support for conference bridges**

Cisco Unified Communications Manager provides annunciator resource support to a conference bridge under the following circumstances:

- If the media resource group list that contains the annunciator is assigned to the device pool where the conference bridge exists.
- If the annunciator is configured as the default media resource.

Cisco Unified Communications Manager does not provide annunciator resource support for a conference bridge if the media resource group list is assigned directly to the device that controls the conference.

**Conference bridge types in Cisco Unified Communications Manager administration**

The following conference bridge types exist in Cisco Unified Communications Manager Administration.
<table>
<thead>
<tr>
<th>Conference Bridge Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Conference Bridge Hardware (WS-6608-T1 or WS-6608-E1)</td>
<td>This type supports the Cisco Catalyst 4000 and 6000 Voice Gateway Modules and the following number of conference sessions.</td>
</tr>
<tr>
<td></td>
<td><strong>Cisco Catalyst 6000</strong></td>
</tr>
<tr>
<td></td>
<td>• G.711 or G.729a conference-32 participants per port; six participants maximum per conference; 256 total participants per module; 10 bridges with three participants</td>
</tr>
<tr>
<td></td>
<td>• GSM-24 participants per port; six participants maximum per conference; 192 total participants per module</td>
</tr>
<tr>
<td></td>
<td><strong>Cisco Catalyst 4000</strong></td>
</tr>
<tr>
<td></td>
<td>• G.711 conference only-24 conference participants; maximum of four conferences with six participants each</td>
</tr>
<tr>
<td>Cisco Conference Bridge Software</td>
<td>Software conference devices support G.711 codecs by default. The maximum number of audio streams for this type equals 128. With 128 streams, a software conference media resource can handle 128 users in a single conference, or the software conference media resource can handle up to 42 conferencing resources with three users per conference. Caution If the Cisco IP Voice Media Streaming Application service runs on the same server as the Cisco CallManager service, a software conference should not exceed the maximum limit of 48 participants.</td>
</tr>
<tr>
<td>Cisco IOS Conferencing and Transcoding for Voice Gateway Routers</td>
<td>• Uses the NM-HDV or NM-HDV-FARM network modules.</td>
</tr>
<tr>
<td></td>
<td>• G.711 a/mu-law, G.729, G.729a, G.729b, and G.729ab participants joined in a single conference</td>
</tr>
<tr>
<td></td>
<td>• Up to six parties joined in a single conference call</td>
</tr>
<tr>
<td></td>
<td>Cisco Unified Communications Manager assigns conference resources to calls on a dynamic basis. In a Cisco Unified Communications Manager network that includes both Cisco IOS Conferencing and Cisco IOS Enhanced Conferencing, set the Cisco CallManager service parameters, Maximum Ad hoc Conference and the Maximum MeetMe Conference Unicast, to six conference participants. For more information about Cisco IOS Conferencing and Transcoding for Voice Gateway Routers, see the IOS documentation that you received with this product.</td>
</tr>
</tbody>
</table>
### Conference Bridge Type

<table>
<thead>
<tr>
<th>Conference Bridge Type</th>
<th>Description</th>
</tr>
</thead>
</table>
| Cisco IOS Enhanced Conferencing and Transcoding for Voice Gateway Routers             | • Uses the onboard Cisco Packet Voice/Fax Digital Signal Processor Modules (PVDM2) on the Cisco 2800 and 3800 series voice gateway routers or uses the NM-HD or NM-HDV2 network modules.  
• G.711 a-law/mu-law, G.729, G.729a, G.729b, G.729ab, GSM FR, and GSM EFR participants joined in a single conference  
• Up to eight parties joined in a single call.  
**Tip** In Cisco Unified Communications Manager Administration, ensure that you enter the same conference bridge name that exists in the gateway Command Line Interface.  
Cisco Unified Communications Manager assigns conference resources to calls on a dynamic basis. In a Cisco Unified Communications Manager network that includes both Cisco IOS Conferencing and Cisco IOS Enhanced Conferencing, set the Cisco CallManager service parameters, Maximum Ad hoc Conference and the Maximum MeetMe Conference Unicast, to six conference participants.  
For more information about Cisco IOS Enhanced Conferencing and Transcoding for Voice Gateway Routers, see the IOS documentation that you received with this product. |
| Cisco Video Conference Bridge (IPVC-35xx)                                            | This conference bridge type specifies a dual multimedia bridge that provides video conferencing. The Cisco Video Conference Bridge provides audio and video conferencing functions for Cisco IP video phones, H.323 endpoints, and audio-only Cisco Unified IP Phones. |
| Cisco Conference Bridge (WS-SVC-CMM)                                                 | This conference bridge type supports the Cisco Catalyst 6500 series and Cisco 7600 series Communication Media Module (CMM).  
This conference bridge type supports up to eight parties per conference and up to 64 conferences per port adapter. This conference bridge type supports the following codecs: G.711 mu-law, G.711 a-law, G.729 annex A and annex B, and G.723.1. This conference bridge type supports ad hoc conferencing. |
<table>
<thead>
<tr>
<th>Conference Bridge Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS Homogeneous Video Conference Bridge</td>
<td>Cisco Integrated Services Routers Generation 2 (ISR G2) can act as IOS-based conference bridges that support ad hoc and meet-me video conferencing. DSP modules must be installed on the router to enable the router as a conference bridge. Cisco IOS Homogeneous Video Conference Bridge specifies the IOS-based conference bridge type that supports homogeneous video conferencing. A homogeneous video conference is a video conference in which all participants connect using the same video format attributes. All the video phones support the same video format and the conference bridge sends the same data stream format to all the video participants. If the conference bridge is not configured to support the video format of a phone, the caller on that phone connects to the conference as an audio only participant. For more detailed information about video conferencing with ISR G2 routers, refer to the document Configuring Video Conferences and Video Transcoding.</td>
</tr>
</tbody>
</table>
| Cisco IOS Heterogeneous Video Conference Bridge | Cisco Integrated Services Routers Generation 2 (ISR G2) can act as IOS-based conference bridges that support ad hoc and meet-me video conferencing. DSP modules must be installed on the router to enable the router as a conference bridge. Cisco IOS Heterogeneous Video Conference Bridge specifies the IOS-based conference bridge type that supports heterogeneous video conferences. In a heterogeneous video conference, all the conference participants connect to the conference bridge with phones that use different video format attributes. In heterogeneous conferences, transcoding and transsizing features are required from the DSP to convert the signal between the various formats. For heterogeneous video conferences, callers connect to the conference as audio participants under either of the following conditions:  
  • Insufficient DSP resources.  
  • The conference bridge is not configured to support the video capabilities of the phone. For more detailed information about video conferencing with ISR G2 routers, refer to the document Configuring Video Conferences and Video Transcoding. |
### Conference Bridge Type

<table>
<thead>
<tr>
<th>Conference Bridge Type</th>
<th>Description</th>
</tr>
</thead>
</table>
| Cisco Guaranteed Audio Video Conference Bridge | Cisco Integrated Services Routers Generation 2 (ISR G2) can act as IOS-based conference bridges that support ad hoc and meet-me voice and video conferencing. DSP modules must be installed on the router to enable the router as a conference bridge.  
Cisco IOS Guaranteed Audio Video Conference Bridge specifies the IOS-based video conference bridge type where DSP resources are reserved for the audio portion of the conference, and video service is not guaranteed. Callers on video phones may have video service if DSP resources are available at the start of the conference. Otherwise, the callers connect to the conference as audio participants.  
For more detailed information about video conferencing with ISR G2 routers, refer to the document Configuring Video Conferences and Video Transcoding. |
| Cisco TelePresence MCU                  | Cisco TelePresence MCU is a set of hardware conference bridges for Cisco Unified Communications Manager.  
The Cisco TelePresence MCU is a high-definition (HD) multipoint video conferencing bridge. It delivers up to 1080p at 30 frames per second, full continuous presence for all conferences, full transcoding, and is ideal for mixed HD endpoint environments.  
The Cisco TelePresence MCU supports SIP as the signaling call control protocol. It has a built in Web Server that allows for complete configuration, control, and monitoring of the system and conferences. The Cisco TelePresence MCU provides XML management API over HTTP.  
Cisco TelePresence MCU allows both ad hoc and meet-me voice and video conferencing. Each conference bridge can host several simultaneous, multiparty conferences.  
Cisco TelePresence MCU must be configured in Port Reservation mode. For more information, consult the Cisco TelePresence MCU Configuration Guide.  
**Note** Cisco TelePresence MCU does not support a common out-of-band DTMF method. Under the default setting, Cisco Unified Communications Manager will not require an MTP. However, if the Media Termination Point Required check box is checked, Cisco Unified Communications Manager will allocate an MTP and the SIP trunk will negotiate DTMF according to RFC 2833.  
**Note** BFCP is not supported when used between Cisco Unified Communications Manager and Cisco TelePresence MCU.  
**Note** TLS is not supported with Cisco TelePresence MCU. |
Conference types

Cisco Unified Communications Manager supports both meet-me conferences and ad hoc conferences. Meet-me conferences allow users to dial in to a conference. Ad hoc conferences allow the conference controller (or in some cases, another participant) to add specific participants to the conference.

Meet-me conferences require that a range of directory numbers be allocated for exclusive use of the conference. When a meet-me conference is set up, the conference controller chooses a directory number and advertises it to members of the group. The users call the directory number to join the conference. Anyone who calls the directory number while the conference is active joins the conference. (This situation applies only when the maximum number of participants that is specified for that conference type has not been exceeded and when sufficient streams are available on the conference device.)

Ad hoc conferences comprise two types: basic and advanced. In basic ad hoc conferencing, the originator of the conference acts as the controller of the conference and is the only participant who can add or remove other participants. In advanced ad hoc conferencing, any participant can add or remove other participants; that capability does not get limited to the originator of the conference. Advanced ad hoc conferencing also allows you to link multiple ad hoc conferences together. Set the Advanced Ad Hoc Conference Enabled clusterwide service parameter to True to gain access to advanced ad hoc conferencing.

Initiate an ad hoc conference

Initiate ad hoc conferences in the following ways:

- Press the Conference (Confrn) softkey, dial another participant, and press the Confrn softkey again to add the new participant.
- Join established calls by using the Select and Join softkeys.

If sufficient streams are available on the conference device, the conference controller (or other participant in the case of advanced ad hoc conferencing) can add up to the maximum number of participants that is specified for ad hoc conferences to the conference. Configure the maximum number of participants for an ad hoc conference with the Maximum Ad Hoc Conference service parameter in the Service Parameter Configuration window. Cisco Unified Communications Manager supports multiple, concurrent ad hoc conferences on each line appearance of a device.

Using Conference Softkey for an Ad Hoc Conference

When a user initiates a conference call, Cisco Unified Communications Manager places the current call on hold, flashes the conference lamp (if applicable), and provides dial tone to the user. At the dial tone, the conference controller dials the next conference participant and presses the Conference softkey to complete the conference. Cisco Unified Communications Manager then connects the conference controller, the first participant, and the new conference participant to a conference bridge. Each participating Cisco Unified IP Phone display reflects the connection to the conference.

The conference controller (or other participant in the case of advanced ad hoc conferencing) can drop the last conference participant from the conference by pressing the RmLstC softkey on the Cisco Unified IP Phone 7960 or 7940. The conference controller (or other participant in the case of advanced ad hoc conferencing) can also remove any conference participant by pressing the ConfList softkey to display the list of participants, highlighting a participant, and pressing the Remove softkey (only visible after you press the ConfList softkey).

A conference participant can view the list of conference participants by pressing the Conference List (ConfList) softkey and can drop the last conference participant from the conference by pressing the Remove Last Conference Party (RmLstC) softkey on the Cisco Unified IP Phone. If a conference participant transfers the
conference to another party, the transferred party becomes the last conference participant in the conference. If a conference participant parks the conference, the participant becomes the last party in the conference when the participant picks up the conference. When only two participants remain in the conference, Cisco Unified Communications Manager terminates the conference, and the two remaining participants reconnect directly as a point-to-point call.

Participants can leave a conference by simply hanging up. In basic ad hoc conferencing, a conference continues even if the conference controller hangs up, although the remaining conference participants cannot add new participants to the conference. In advanced ad hoc conferencing, a conference continues even if the originator hangs up, and any remaining participant can add new participants.

Conference by Using **Join** Softkey

The user initiates an ad hoc conference by using the Select and Join softkeys. During an established call, the user chooses conference participants by pressing the **Select** softkey and then presses the **Join** softkey, making it an ad hoc conference. Up to 15 established calls can be added to the ad hoc conference, for a total of 16 participants. Cisco Unified Communications Manager treats the ad hoc conference the same way as one that is established by using the Conference softkey method.

---

**Note**

The Join Across Lines feature allows the user to join conference participants across different lines—either on different directory numbers, or on the same directory number but on different partitions. The Maximum Ad Hoc Conference Service Parameter controls the maximum number of established calls that can be added to the conference.

Conference by Using **cBarge**

You can initiate a conference by pressing the **cBarge** softkey, or if the Single Button cBarge feature is enabled, by pressing the shared-line button of the active call. When cBarge is initiated, a barge call gets set up by using the shared conference bridge, if available. The original call gets split and then joined at the conference bridge. The call information for all parties gets changed to Conference.

The barged call becomes a conference call with the barge target device as the conference controller. It can add more parties to the conference or can drop any party.

When any party releases from the call, leaving only two parties in the conference, the remaining two parties experience a brief interruption and then get reconnected as a point-to-point call, which releases the shared conference resource.

---

**Ad hoc conference linking**

Advanced ad hoc conferencing allows you to link multiple ad hoc conferences together by adding an ad hoc conference to another ad hoc conference as if it were an individual participant. If you attempt to link multiple conferences together when the Advanced Ad Hoc Conference Enabled service parameter is set to False, the IP phone displays a message. You can also use the methods that are available for adding individual participants to an ad hoc conference to add another conference to an ad hoc conference.

You can invoke ad hoc conference linking for phones that are running SIP only by using the Conference and Transfer functions. The system does not support Direct Transfer and Join. Supported phones that are running SIP comprise Cisco Unified IP Phones 7911, 7941, 7961, 7970, and 7971.
The participants in linked conferences can all hear and talk with one another, but the conferences do not get merged into a single conference. The Conference List (ConfList) softkey displays an added conference as Conference and does not display the individual participants in the added conference. Each participant can see only the individual participants in their own conference bridge.

Note

Two types of conference linking exist: linear and nonlinear.

Linear Ad Hoc Conference Linking

In linear ad hoc conference linking, no more than two ad hoc conferences can link directly to any participating conference. The following figure is an example of linear ad hoc conference linking.

Figure 31: Linear Ad Hoc Conference Linking Example

With linear conference linking, no limitation exists to the number of ad hoc conferences that can be added, as long as no more than two conferences link directly to any one conference.

Caution

If Conference Bridge 1 links directly to Conference Bridge 3, a looped conference results. Looping conferences do not add any functionality, and Cisco recommends avoiding them because participants in all the conferences can hear echoes.
**Nonlinear Ad Hoc Conference Linking**

When three or more ad hoc conferences link directly to another conference, nonlinear linking results. The system does not permit this type of linking by default because potentially negative impact on conference resources exists. See the following figure for an example of nonlinear ad hoc conference linking.

*Figure 32: Nonlinear Ad Hoc Conference Linking Example*

![Diagram of nonlinear ad hoc conference linking](image)

To enable nonlinear conference linking, set the Non-linear Ad Hoc Conference Linking Enabled clusterwide service parameter to True. Non-linear ad hoc conference linking will not work unless you set both the Non-linear Ad Hoc Conference Linking Enabled and Advanced Ad Hoc Conference Enabled service parameters to True.

You can access the Non-linear Ad Hoc Conference Linking Enabled service parameter only in the Advanced view of the Service Parameters Configuration window.

**Note**

Keep the Non-linear Ad Hoc Conference Linking Enabled service parameter set to the default value (False) unless a Cisco support engineer instructs otherwise.

**Caution**

When conferences are linked in nonlinear fashion, the conference resources may not get released when all real participants have dropped out of the conference, which leaves the conference bridges connected to each other when no one is using them. This can happen because each conference only recognizes the participants that connect directly to its own conference bridge. They cannot detect when all the real participants in the other conferences have dropped out. To reduce the risk of tying up conference resources, restart conference bridges more frequently when the Non-linear Ad Hoc Conference Linking Enabled service parameter is set to True.

**Ad hoc conference settings**

Three clusterwide service parameters affect ad hoc conferencing:
• Drop Ad Hoc Conference
• Advanced Ad Hoc Conference Enabled
• Non-linear Ad Hoc Conference Linking Enabled

Drop ad hoc conference

The Drop Ad Hoc Conference parameter allows you to choose when to drop an ad hoc conference.

To use the additional functionality that advanced ad hoc conferencing provides, Cisco recommends that you set this service parameter to Never. Any other setting can result in unintentional termination of a conference.

Cisco Unified Communications Manager Administration provides the clusterwide service parameter, Drop Ad Hoc Conference, to allow the prevention of toll fraud (where an internal conference controller disconnects from the conference while outside callers remain connected). The service parameter settings specify conditions under which an ad hoc conference gets dropped.

To configure the value of the service parameter, perform the following procedure:

Procedure

Step 1 From Cisco Unified Communications Manager Administration, choose System > Service Parameters.
Step 2 From the Server drop-down list box, choose the server.
Step 3 From the Service drop-down list box, choose Cisco Unified Communications Manager.
Step 4 From the Drop Ad Hoc Conference drop-down list box, which is listed in the Clusterwide Parameters (Features - General) area of the window, choose one of the following options:
   a) Never-The conference does not get dropped. (This represents the default option.)
   b) When No OnNet Parties Remain in the Conference-The system drops the active conference when the last on-network party in the conference hangs up or drops out of the conference. Cisco Unified Communications Manager releases all resources that are assigned to the conference.
   For more information about OnNet and OffNet, see Cisco Unified Communications Manager voice gateways overview, on page 357, Cisco Unified Communications Manager trunk types, on page 449, and Understanding route plans, on page 143
   c) When Conference Controller Leaves-The active conference terminates when the primary controller (conference creator) hangs up. Cisco Unified Communications Manager releases all resources that are assigned to the conference.

   If the conference controller transfers, parks, or redirects the conference to another party, the party that retrieves the call acts as the virtual controller for the conference. A virtual controller cannot add new parties to the conference nor remove any party that was added to the conference, but a virtual controller can transfer, park, or redirect the conference to another party, who would, in turn, become the virtual controller of the conference. When this virtual controller hangs up the call, the conference ends.
Step 5  Click Save.

Note  Cisco Unified Communications Manager does not support multiple selections; that is, all conferences will support the same functionality depending on the option that you choose.

Enable advanced ad hoc conference

The Advanced Ad Hoc Conference Enabled parameter allows you to choose whether advanced ad hoc conferencing functionality is available to users. This includes the ability of non-controller participants to add and remove other participants and the ability of all participants to link ad hoc conferences together.

To configure the value of the service parameter, perform the following procedure:

Procedure

Step 1  From Cisco Unified Communications Manager Administration, choose Service > Service Parameter.
Step 2  From the Server drop-down list box, choose the server.
Step 3  From the Service drop-down list box, choose Cisco Unified Communications Manager.
Step 4  From the Advanced Ad Hoc Conference Enabled drop-down list box, choose one of the following options:
   a) False-This default option specifies that advanced ad hoc conference functionality is not enabled.
   b) True-This option specifies that advanced ad hoc conference functionality is enabled.
Step 5  Click Update.

Enable non-linear ad hoc conference linking

The Non-linear Ad Hoc Conference Linking Enabled parameter allows you to choose whether participants can link conferences in nonlinear fashion (three or more conferences linked to any one conference).

Note  Do not change this setting from the default except with the guidance of a Cisco support engineer.

To configure the value of the service parameter, perform the following procedure:

Procedure

Step 1  From Cisco Unified Communications Manager Administration, choose Service > Service Parameter.
Step 2  From the Server drop-down list box, choose the server.
Step 3  From the Service drop-down list box, choose Cisco Unified Communications Manager.
Step 4  Click the Advanced button near the top of the window.
Step 5  From the Non-linear Ad Hoc Conference Linking Enabled drop-down list box, choose one of the following options:
   a) False-This default option specifies that nonlinear conference linking is not allowed. Do not change this setting from the default except with the guidance of a Cisco support engineer.
Ad hoc conference settings restrictions for phones that are running SIP

The following sections describe the ad hoc conference differences for the Cisco Unified IP Phones that are running SIP.

Ad Hoc Conference Restrictions for Cisco Unified IP Phones 7911, 7941, 7961, 7970 and 7971 that are Running SIP

- Cisco Unified Communications Manager uses “beep” and “beep beep” tones when a new party is added and when the new party drops from the ad hoc conference, respectively. When a party is added to an ad hoc conference, a user on a phone that is running SIP may or may not receive the beep; when a participant drops from the ad hoc conference, a user on a phone that is running SIP may not receive the beep beep. Users might not hear the beeps because of the time it takes Cisco Unified Communications Manager to set up and tear down connections during the conferencing process.

Ad Hoc Conference Restrictions for Cisco Unified IP Phones 7940/7960 that are Running SIP and Third-Party Phones that are Running SIP

- When a local conference is created, the display on a phone that is running SIP display differs from the display on a phone that is running SCCP; for example, phones that are running SCCP display the call as a conference call whereas phones that are running SIP display the calls that are conferenced as individual calls (with a conference icon next to each call). Even though Cisco Unified IP Phone 7940/7960 that is running SIP cannot create an ad hoc conference, it can create a local conference.

- You cannot use Conference list (ConfList), which is not available.

- You cannot use Remove last conference participant (RmLstC), which is not available.

- Because Cisco Unified Communications Manager does not recognize the preceding phones that are running SIP that initiated a conference call as a conference, the Drop Ad Hoc Conference service parameter settings do not apply.

- The SIP Profile parameter, Conference Join Enabled, controls behavior of the phone that is running SIP when the conference controller exits a locally hosted conference. If the Conference Join Enabled check box is unchecked, all legs disconnect when the conference controller exits the ad hoc conference call. If the Conference Join Enabled check box is checked, the remaining two parties stay connected.

- To achieve the same level of control that the Drop Ad Hoc Conference parameter settings provides for conference calls that a phone that is running SCCP initiates, the administrator can use a combination of the Conference Join Enabled SIP profile parameter and the Block OffNet to OffNet Transfer service parameter for conferences that are initiated on the phone that is running SIP (Cisco Unified IP Phone 7940/60). (Because the phone that is running SIP performs a transfer when it drops out of the conference call, the Block OffNet to OffNet Transfer can prevent toll fraud by not allowing two offset phones to remain in the call.)

- Cisco Unified Communications Manager uses “beep” and “beep beep” tones when a new party is added and when the new party drops from the ad hoc conference, respectively. When a party is added to an ad hoc conference, a user on a phone that is running SIP may or may not hear the beep; when a participant
drops from the ad hoc conference, a user on a phone that is running SIP may not hear the beep beep. Users might not hear the beeps because of the time it takes Cisco Unified Communications Manager to set up and tear down connections during the conferencing process.

Ad hoc conference limitations

The following limitations apply to ad hoc conferencing:

- Cisco Unified Communications Manager supports a maximum of 100 simultaneous ad hoc conferences for each Cisco Unified Communications Manager server.

- Cisco Unified Communications Manager supports a maximum of 64 participants per ad hoc conference (provided adequate conference resources are available). In the case of linked ad hoc conferences, the system considers each conference as one participant. This remains true regardless of whether the conferences are linked in linear or nonlinear fashion.

Meet-me conference

Meet-me conferences require that a range of directory numbers be allocated for exclusive use of the conference. When a meet-me conference is set up, the conference controller chooses a directory number and advertises it to members of the group. The users call the directory number to join the conference. Anyone who calls the directory number while the conference is active joins the conference. (This situation applies only when the maximum number of participants that is specified for that conference type has not been exceeded and when sufficient streams are available on the conference device.)

When you initiate a meet-me conference by pressing Meet-Me on the phone, Cisco Unified Communications Manager considers you the conference controller. The conference controller provides the directory number for the conference to all attendees, who can then dial that directory number to join the conference. If other participants in a meet-me conference press Meet-Me and the same directory number for the conference bridge, the Cisco Unified Communications Manager ignores the signals.

The conference controller chooses a directory number from the range that is specified for the Meet-Me Number/Pattern. The Cisco Unified Communications Manager administrator provides the meet-me conference directory number range to users, so they can access the feature.

A meet-me conference continues even if the conference controller hangs up.

Meet-me conference limitations

Cisco Unified Communications Manager supports a maximum of 100 simultaneous meet-me conferences for each Cisco Unified Communications Manager server.

Conferences and the party entrance tone

With the party entrance tone feature, a tone plays on the phone when a basic call changes to a multiparty call; that is, when a basic call changes to a barged call, cBarged call, ad hoc conference, meet-me conference, or a joined call. In addition, a different tone plays when a party leaves the multiparty call.

When a meet-me conference gets created, the party entrance tone configuration for the first party to enter the conference determines whether Cisco Unified Communications Manager plays the tone. Cisco Unified Communications Manager uses the configuration for the first party until the conference ends.
When a joined call or ad hoc conference begins, Cisco Unified Communications Manager uses the party entrance tone configuration from the conference controller. Cisco Unified Communications Manager uses this configuration until the conference ends.

If two ad hoc conferences are chained together and the controlling device for one conference has the party entrance tone set to True while the other controlling device for the other conference has a party entrance tone of False, Cisco Unified Communications Manager determines whether to play the tone based on the conference to which the new party is added.

To use the party entrance feature, ensure that you turned the privacy feature off for the devices and ensure that the controlling device for the multiparty call has a built-in bridge. In addition, either configure the Party Entrance Tone service parameter, which supports the Cisco CallManager service, or configure the Party Entrance Tone setting per directory number in the Directory Number Configuration window. For information on the service parameter, click the question-mark button in the Service Parameter window.

**Intelligent bridge selection**

**Note**
The Intelligent Bridge Selection feature applies only to ad hoc conferences and does not impact how conference bridges are allocated for meet-me conferences. The conference bridge for a meet-me conference is allocated on the basis of the configured Media Resource Group List (MRGL) for the endpoint that initiates the conference. Cisco Unified Communications Manager does not take into account whether the conference initiator is video-capable to allocate a conference bridge for meet-me conference calls.

Cisco Unified Communications Manager can intelligently select a video conference bridge from the configured MRGL if two or more of the original conference participants are video enabled. If only one or no video participants exist, Cisco Unified Communications Manager selects an audio conference bridge from the configured MRGL.

Cisco Unified Communications Manager selects an audio or a video conference bridge from the configured MRGL of the conference initiator. However, if no MRGL is configured for the conference initiator, Cisco Unified Communications Manager allocates the video or audio conference bridge from the default MRGL.

**Note**
Any conference resource that is not added to a media resource group becomes a part of the default MRGL and is available to everyone.

If a video conference bridge needs to be allocated but none is available, Cisco Unified Communications Manager allocates an audio conference bridge for the conference. Similarly, if an audio conference bridge is needed but is unavailable, Cisco Unified Communications Manager allocates a video conference bridge.

**Note**
Certain endpoints, like a phone that is running SCCP with CUVA installed, may report that they are not video capable if the phone is not configured for video capability (though Cisco Unified Communications Manager Administration) or if the CUVA application is not running.

When a conference is established by using an audio bridge and then additional video-capable participants join the conference, the conference remains on the audio bridge and does not transfer to a video bridge. Similarly,
when the conference is established on a video conference bridge and video capable participants drop out, the conference does not convert to an audio conference bridge.

Note
In certain shared-line cases, the video capability that is used might not be accurate. For example, when a blind conference call rings on two shared-line devices, video capability gets used from the device that rings first.

If the endpoints that are joining the conference are video capable but not enough bandwidth exists to support a video conference in the region where the devices are located, and the region where conference bridge is; a video conference bridge gets allocated if one exists in the configured MRGL of the conference initiator. However, the devices cannot take advantage of the video capability of the conference bridge, and a video cannot be exchanged between them.

The System supports Intelligent Bridge Selection feature for both inter cluster calls over SIP, and H323 ICT and intracluster calls.

Note
The video conference bridge gets allocated on the basis of the video capability of the endpoints and the MRGL that is configured for the conference initiator. As long as the device capability is correctly reported to Cisco Unified Communications Manager, it can allocate appropriate conference resources.

Configure intelligent bridge selection
You can change the default behavior of Intelligent Bridge Selection by configuring the service parameters in this section.

Choose encrypted audio conference Instead of video conference
This parameter determines whether Cisco Unified Communications Manager chooses an encrypted audio conference bridge or an unencrypted video conference bridge for an ad hoc conference call, when

• The conference controller Device Security Mode is set to either Authenticated or Encrypted
• At least two conference participants are video-capable

Because no encrypted video conference bridges exist, Cisco Unified Communications Manager chooses between an encrypted audio conference bridge and an unencrypted video conference bridge.

Valid values specify

• True: Cisco Unified Communications Manager allocates an encrypted audio conference bridge instead of video

OR

• False: Cisco Unified Communications Manager allocates an unencrypted video conference bridge.

The default value for this parameter specifies True.
Minimum video-capable participants to allocate video conference

This parameter specifies the number of video-capable conference participants that must be present in an ad hoc conference for Cisco Unified Communications Manager to allocate a video conference bridge. If the number of video-capable participants is fewer than the number that this parameter specifies, Cisco Unified Communications Manager allocates an audio conference bridge. If the number of video-capable participants equals to or is greater than the number that this parameter specifies, Cisco Unified Communications Manager allocates a video conference bridge, when available, from the configured media resource group list (MRGL).

Specifying a value of 0 means that a video conference bridge will always be allocated, even when none of the participants on the conference is video-capable.

The default value for this service parameter specifies 2. The minimum value specifies 0 and the maximum value specifies 10.

Allocate video conference bridge for audio-only conferences when video conference bridge has higher priority

This parameter determines whether Cisco Unified Communications Manager chooses a video conference bridge, when available, for an ad hoc audio-only conference call when a video conference bridge has a higher priority than an audio conference bridge in the MRGL.

If an audio conference bridge has higher priority than any video conference bridge in the MRGL, Cisco Unified Communications Manager ignores this parameter.

This parameter proves useful in situations where the local conference bridge is a video bridge (and configured in the MRGL with the highest priority) and audio conference bridges are only available in remote locations. In such a situation, enabling this parameter enables Cisco Unified Communications Manager to attempt to use the local video conference bridge first, even for audio-only conference calls.

Valid values specify

• True: Cisco Unified Communications Manager allocates a video conference bridge from the MRGL

OR

• False: Cisco Unified Communications Manager allocates an audio conference bridge from the MRGL.

The default value for this service parameter specifies False.

Note

This parameter is visible under the Advanced options.

Limitations of intelligent bridge selection

The limitations of intelligent bridge selection are described in this section.

Blind conference over SIP ICT

The Intelligent Bridge Selection feature assumes that the video capability of each device joining the conference is available prior to conference getting setup. However, for a conference over SIP ICT, the device capability of the far end is not available until media connect time. Therefore, when a blind conference is initiated, the
video capability of only two endpoints is available and this can cause an incorrect conference bridge to be allocated.

Consider the following scenario to understand this limitation:

**Example Scenario**

1. Video Endpoint (CCM1) calls Audio Endpoint (CCM1).
2. The Audio Endpoint (CCM1) presses the “Confm” softkey and then calls a Video Endpoint (CCM2) over SIP ICT.
3. The Audio Endpoint then presses the “Confm” softkey again before Video Endpoint (CCM2) answers the call.

**Result**

The conference gets created and an audio conference bridge gets allocated even though there are two video endpoints in the conference. This is because the video capability of Video Endpoint (CCM2) is not available when the conference is created.

**Conference over H323 ICT**

If an audio endpoint calls a video endpoint over H323 ICT, the video endpoint reports its capabilities as audio only, instead of video. Therefore, if a conference is now setup using another video endpoint, Intelligent Bridge Selection feature assumes that there is only 1 video endpoint and this causes an incorrect conference bridge to be allocated.

Consider the following scenario to understand this limitation:

**Example Scenario**

1. A Video Endpoint (CCM1) calls Audio Endpoint (CCM1).
2. The Audio Endpoint (CCM1) presses the “Confm” softkey and then calls a Video Endpoint (CCM2) over H323 ICT.
3. After the Video Endpoint (CCM2) answers the call, Audio Endpoint (CCM1) presses the “Confm” softkey again.

**Result**

The conference gets created and an audio conference bridge gets allocated even though there are two video endpoints in the conference. This is because the Video Endpoint (CCM2) reports itself as audio capable only, because it is talking to another audio endpoint (CCM1).

However, if the capability of endpoints is switched so that the Video Endpoint (CCM1) calls an Audio Endpoint (CCM2), the system allocates the correct conference bridge.

**Dependency records**

To find out which media resource groups are associated with a conference bridge, click the Dependency Records link that is provided on the Cisco Unified Communications Manager Administration Conference Bridge Configuration window. The Dependency Records Summary window displays information about media
resource groups that are using the conference bridge. To find out more information about the media resource
group, click the media resource group, and the Dependency Records Details window displays. If the dependency
records are not enabled for the system, the dependency records summary window displays a message.

Conference bridge performance monitoring and troubleshooting

The Real Time Monitoring Tool counters for conference bridges allow you to monitor the number of conference
bridges that are currently registered with the Cisco Unified Communications Manager but are not currently
in use, the number of conferences that are currently in use, the number of times that a conference completed,
and the number of times that a conference was requested for a call but no resources were available.

For more information about Real Time Monitoring Tool counters, see the Cisco Unified Serviceability
Administration Guide.

Cisco Unified Communications Manager writes all errors for conference bridges to the Local SysLog Viewer
in the Real Time Monitoring Tool. In Cisco Unified Serviceability, you can set traces for the Cisco IP Voice
Media Streaming Application service (using Trace Configuration); to troubleshoot most issues, you must
choose the Significant or Detailed option for the service, not the Error option. After you troubleshoot the
issue, change the Debug Trace Level back to the Error option.

Cisco Unified Communications Manager generates registration and connection alarms for conference bridges
in Cisco Unified Serviceability. For more information on alarms, see the Cisco Unified Serviceability
Administration Guide.

If you need technical assistance, use the following CLI commands to locate the conference bridge logs:

```
file list activelog cm/trace/cms/sdi/*.txt
file get activelog cm/trace/cms/sdi/*.txt
file view activelog cm/trace/cms/sdi/cms00000000.txt
file tail activelog cm/trace/cms/sdi/cms00000000.txt
```

Locate the logs before you contact your Cisco Partner or the Cisco Technical Assistance Center (TAC).
Transcoders

This chapter provides information about transcoders. The Media Resource Manager (MRM) provides resource reservation of transcoders. Cisco Unified Communications Manager supports simultaneous registration of both the media termination point (MTP)/trusted relay point (TRP) and transcoder and concurrent MTP/TRP and transcoder functionality within a single call.

- Configure transcoder, page 287
- Transcoders overview, page 288
- Transcoder failover and fallback, page 291
- Dependency records, page 292
- Transcoder performance monitoring and troubleshooting, page 292

Configure transcoder

A transcoder takes the media stream of one codec and transcodes (converts) it from one compression type to another compression type. For example, it could take a stream from a G.711 codec and transcode (convert) it in real time to a G.729 stream. In addition to codec conversion, a transcoder resource can also provide MTP/TRP functionality to a call.

The Cisco Unified Communications Manager invokes a transcoder on behalf of endpoint devices when the two devices use different voice codecs and would normally not be able to communicate. When inserted into a call, the transcoder converts the data streams between the two incompatible codecs to enable communications between them. The transcoder remains invisible to either the user or the endpoints that are involved in a call.

A transcoder provides a designated number of streaming mechanisms, each of which can transcode data streams between different codecs.

To configure transcoders, refer to the following steps.
Procedure

**Step 1** Determine the number of transcoder resources that are needed and the number of transcoder devices that are needed to provide these resources.

**Step 2** Add and configure the transcoders.

**Step 3** Add the new transcoders to the appropriate media resource groups.

**Step 4** Restart the transcoder device.

Related Topics

- Media resource management, on page 245

## Transcoders overview

A transcoder takes the media stream of one codec and transcodes (converts) it from one compression type to another compression type. For example, it could take a stream from a G.711 codec and transcode (convert) it in real time to a G.729 stream. In addition to codec conversion, a transcoder resource can also provide MTP/TRP functionality to a call.

The Cisco Unified Communications Manager invokes a transcoder on behalf of endpoint devices when the two devices use different voice codecs and would normally not be able to communicate. When inserted into a call, the transcoder converts the data streams between the two incompatible codecs to enable communications between them. The transcoder remains invisible to either the user or the endpoints that are involved in a call.

A transcoder provides a designated number of streaming mechanisms, each of which can transcode data streams between different codecs.

### Manage transcoders with the Media Resource Manager

All Cisco Unified Communications Managers can access transcoders through the Media Resource Manager (MRM). The MRM manages access to transcoders.

The MRM makes use of Cisco Unified Communications Manager media resource groups and media resource group lists. The media resource group list allows transcoders to communicate with other devices in the assigned media resource group, which in turn, provides management of resources within a cluster.

A transcoder control process gets created for each transcoder device that is defined in the database. The MRM keeps track of the transcoder resources and advertises their availability.

### Use transcoders as MTPs

Hardware-based transcoder resources also support MTP and/or TRP functionality. In this capacity, when the Cisco Unified Communications Manager determines that an endpoint in a call requires an MTP or TRP, it can allocate a transcoder resource and inserts it into the call, where it acts like an MTP transcoder.

Cisco Unified Communications Manager supports MTP and TRP and transcoding functionality simultaneously. For example, if a call originates from a Cisco Unified IP Phone (located in the G723 region) to NetMeeting
(located in the G711 region), one transcoder resource supports MTP and transcoding functionality simultaneously.

If a software MTP resource is not available when it is needed, the call tries to connect without using an MTP resource and MTP/TRP services. If hardware transcoder functionality is required (to convert one codec to another) and a transcoder is not available, the call will fail.

Transcoders and call throttling

The MTP and Transcoder Resource Throttling Percentage service parameter, which supports the Cisco CallManager service, defines a percentage of the configured number of MTP or transcoder resources and allows Cisco Unified Communications Manager to extend the call to an MTP/transcoder that offers the best chance of successfully connecting the call. When the number of active MTP or transcoder resources is equal to or greater than the percentage that is configured for this parameter, Cisco Unified Communications Manager throttles (stops sending) calls to this MTP/transcoder. Cisco Unified Communications Manager hunts through the Media Resource Group List (MRGL) one time to find a MTP/transcoder that uses matching codecs on both sides of the call. If Cisco Unified Communications Manager cannot find an available MTP/transcoder with matching codecs, Cisco Unified Communications Manager returns to the top of the MRGL to repeat the search, which then includes those MTPs/transcoders that are in a throttled state and that match a smaller subset of capabilities for the call. Cisco Unified Communications Manager extends the call to the MTP/transcoder that is the best match for the call when Cisco Unified Communications Manager determines that a resource may be available; the call fails when the MTP/transcoder cannot allocate a resource for the call. In some cases, Cisco Unified Communications Manager perceives that a resource on a hardware MTP/transcoder is available, but the actual port on the hardware is not available.

For example, if you enter 40 for the Call Count service parameter, which supports the Cisco IP Voice Media Streaming Application service, for a software MTP or transcoder (or for hardware resources, if the maximum sessions is configured at 40, for example), and you set the MTP and Transcoder Resource Throttling Percentage service parameter to 95 percent, Cisco Unified Communications Manager throttles calls to the MTP/transcoder when 38 resources are used on this MTP/transcoder (.95 x 40 = 38). When a new request for an MTP or transcoder arrives, Cisco Unified Communications Manager checks whether the number of resources has dropped to 38 or less, and if so, extends the call to the MTP/transcoder.

For the maximum, minimum, and default values for this service parameter, click the question mark help in the Service Parameter Configuration window in Cisco Unified Communications Manager Administration.

Transcoder types in Cisco Unified Communications Manager administration

Transcoder types in Cisco Unified Communications Manager Administration are as follows.
## Table 26: Transcoder Types

<table>
<thead>
<tr>
<th>Transcoder Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Media Termination Point Hardware</td>
<td>This type, which supports the Cisco Catalyst 4000 WS-X4604-GWY and the Cisco Catalyst 6000 WS-6608-T1 or WS-6608-E1, provides the following number of transcoding sessions:</td>
</tr>
<tr>
<td></td>
<td>For the Cisco Catalyst 4000 WS-X4604-GWY</td>
</tr>
<tr>
<td></td>
<td>• For transcoding to G.711-16 MTP transcoding sessions</td>
</tr>
<tr>
<td></td>
<td>For the Cisco Catalyst 6000 WS-6608-T1 or WS-6608-E1</td>
</tr>
<tr>
<td></td>
<td>• For transcoding from G.723 to G.711/For transcoding from G.729 to G.711-24 MTP transcoding sessions per physical port; 192 sessions per module</td>
</tr>
<tr>
<td>Cisco IOS Media Termination Point (hardware)</td>
<td>This type, which supports the Cisco 2600XM, Cisco 2691, Cisco 3725, Cisco 3745, Cisco 3660, Cisco 3640, Cisco 3620, Cisco 2600, and Cisco VG200 gateways, provides the following number of transcoding sessions:</td>
</tr>
<tr>
<td></td>
<td>Per NM-HDV</td>
</tr>
<tr>
<td></td>
<td>• Transcoding from G.711 to G.729-60</td>
</tr>
<tr>
<td></td>
<td>• Transcoding from G.711 to GSM FR/GSM EFR-45</td>
</tr>
<tr>
<td>Cisco IOS Enhanced Media Termination Point (hardware)</td>
<td>This type, which supports Cisco 2600XM, Cisco 2691, Cisco 3660, Cisco 3725, Cisco 3745, and Cisco 3660 Access Routers, provides the following number of transcoding sessions:</td>
</tr>
<tr>
<td></td>
<td>Per NM-HDV</td>
</tr>
<tr>
<td></td>
<td>• Transcoding for G.711 to G.729a/G.729ab/GSMFR-24</td>
</tr>
<tr>
<td></td>
<td>• Transcoding for G.711 to G.729/G.729b/GSM EFR-18</td>
</tr>
<tr>
<td></td>
<td>Per NM-HDV2</td>
</tr>
<tr>
<td></td>
<td>This type, which supports Cisco 2600XM, Cisco 2691, Cisco 3725, Cisco 3745, and Cisco 3660 Access Routers, provides the following number of transcoding sessions:</td>
</tr>
<tr>
<td></td>
<td>• Transcoding for G.711 to G.729a/G.729ab/GSMFR-128</td>
</tr>
<tr>
<td></td>
<td>• Transcoding for G.711 to G.729/G.729b/GSM EFR-96</td>
</tr>
<tr>
<td>Transcoder Type</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| Cisco Media Termination Point (WS-SVC-CMM) | This type provides 64 transcoding sessions per daughter card that is populated: 64 transcoding sessions with one daughter card, 128 transcoding sessions with two daughter cards, 192 transcoding sessions with three daughter cards, and 256 transcoding sessions with four daughter cards (maximum). This type provides transcoding between any combination of the following codecs:  
  - G.711 a-law and G.711 mu-law  
  - G.729 annex A and annex B  
  - G.723.1  
  - GSM (FR)  
  - GSM (EFR) |

Transcoder failover and fallback

This section describes how transcoding devices failover and fallback when the Cisco Unified Communications Manager to which they are registered becomes unreachable. The section also explains conditions that can affect calls that are associated with a transcoding device, such as transcoding 1 reset or restart.

Active Cisco Unified Communications Manager becomes inactive

The following items describe the transcoding device recovery methods when the transcoding device is registered to a Cisco Unified Communications Manager that goes inactive:

- If the primary Cisco Unified Communications Manager fails, the transcoding attempts to register with the next available Cisco Unified Communications Manager in the Cisco Unified Communications Manager Group that is specified for the device pool to which the transcoding belongs.

- The transcoding device reregisters with the primary Cisco Unified Communications Manager as soon as Cisco Unified Communications Manager becomes available.

- A transcoding device unregisters with a Cisco Unified Communications Manager that becomes unreachable. The calls that were on that Cisco Unified Communications Manager will register with the next Cisco Unified Communications Manager in the list.

- If a transcoding device attempts to register with a new Cisco Unified Communications Manager and the registration acknowledgment is never received, the transcoding registers with the next Cisco Unified Communications Manager.

Reset registered transcoding devices

The transcoding devices will unregister and then disconnect after a hard or soft reset. After the reset completes, the devices reregister with the primary Cisco Unified Communications Manager.
Dependency records

To find out which media resources are associated with a transcoder, choose Dependency Records from the Related Links drop-down list box from the Cisco Unified Communications Manager Administration Transcoder Configuration window. Click Go. The Dependency Records Summary window displays information about media resource groups that are using the transcoder. To find out more information about the media resource group, click the media resource group, and the Dependency Records Details window displays. If the dependency records are not enabled for the system, the dependency records summary window displays a message.

Transcoder performance monitoring and troubleshooting

Microsoft Performance Monitor counters for transcoders allow you to monitor the number of transcoders that are currently in use, the number of transcoders that are currently registered with the Cisco Unified Communications Manager but are not currently in use, and the number of times that a transcoder was requested for a call, but no resources were available.

For more information about performance monitor counters, see the Cisco Unified Serviceability Administration Guide.

Cisco Unified Communications Manager writes all errors for the transcoder to the Event Viewer. In Cisco Unified Serviceability, you can set traces for the Cisco IP Voice Media Streaming Application service; to troubleshoot most issues, you must choose the Significant or Detailed option for the service, not the Error option. After you troubleshoot the issue, change the service option back to the Error option.

For more information about the Cisco IP Voice Media Streaming Application service, see the Cisco Unified Serviceability Administration Guide.

Cisco Unified Communications Manager generates registration and connection alarms for transcoder in Cisco Unified Serviceability. For more information on alarms, see the Cisco Unified Serviceability Administration Guide.
Music on hold

This chapter provides information about the integrated Music On Hold (MOH) feature which allows users to place on-net and off-net users on hold with music that is streamed from a streaming source. The Music On Hold feature allows two types of hold:

- End-user hold
- Network hold, which includes transfer hold, conference hold, and call park hold

Music On Hold also supports other scenarios where recorded or live audio is needed.
Media Termination Points

This chapter provides information about Media Termination Point (MTP) software devices which allow Cisco Unified Communications Manager to relay calls that are routed through SIP or H.323 endpoints or gateways.

Note
For information on hardware MTP, which act as transcoders, see the Transcoders, on page 287.

- Configure software MTP, page 295
- Media Termination Points overview, page 296
- Manage MTPs with the Media Resource Manager, page 297
- MTPs and Call Throttling, page 297
- MTP types in Cisco Unified Communications Manager administration, page 298
- Plan software MTP, page 298
- MTP system requirements and limitations, page 300
- MTP failover and fallback, page 300
- Dependency records, page 301
- Software MTP performance monitoring and troubleshooting, page 301

Configure software MTP

A Media Termination Point (MTP) software device allows Cisco Unified Communications Manager to relay calls that are routed through SIP or H.323 endpoints or gateways.

To configure MTP refer to the following steps.
Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Determine the number of MTP resources that are needed and the number of MTP devices that are needed to provide these resources.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Verify that the Cisco IP Voice Media Streaming Application service is activated and running on the server to which you are adding an MTP.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Add and configure the MTPs.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Add the new MTPs to the appropriate media resource groups.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Restart the MTP device.</td>
</tr>
</tbody>
</table>

Related Topics

- Media resource management, on page 245

Media Termination Points overview

Media Termination Points extend supplementary services, such as call hold, call transfer, call park, and conferencing, that are otherwise not available when a call is routed to an H.323 endpoint. Some H.323 gateways may require that calls use an MTP to enable supplementary call services, but normally, Cisco IOS gateways do not. For H.323 supplementary services, MTPs are only required for endpoints that do not support Empty Capability Set (ECS) or FastStart. All Cisco endpoints and most other endpoints do support ECS and FastStart, so an MTP is not required for them.

MTP resources accept two full-duplex G.711 Coder-Decoder (CODEC) stream connections. MTPs bridge the media streams between two connections. The streaming data that is received from the input stream on one connection passes to the output stream on the other connection and vice versa. In addition, the MTP transcodes a-law to mu-law (and vice versa) and adjusts packet sizes as required by the two connections.

Each MTP belongs to a device pool, which specifies, in priority order, the list of Cisco Unified Communications Managers to which the devices that are members of the device pool should attempt to register. This list represents a Cisco Unified Communications Manager group. The first Cisco Unified Communications Manager in the list specifies a device primary Cisco Unified Communications Manager.

An MTP device always registers with its primary Cisco Unified Communications Manager if that Cisco Unified Communications Manager is available and informs the Cisco Unified Communications Manager about how many MTP resources it supports. The Cisco Unified Communications Manager controls MTP resources. You can register multiple MTPs with the same Cisco Unified Communications Manager. When more than one MTP is registered with a given Cisco Unified Communications Manager, that Cisco Unified Communications Manager controls the set of resources for each MTP. You can also distribute the MTPs across a networked system as desired.

For example, consider MTP server 1 as configured for 48 MTP resources, and the MTP server 2 as configured for 24 resources. If both MTPs register with the same Cisco Unified Communications Manager, that Cisco Unified Communications Manager maintains both sets of resources for a total of 72 registered MTP resources.

When the Cisco Unified Communications Manager determines that a call endpoint requires an MTP, it allocates an MTP resource from the MTP that has the least active streams. That MTP resource gets inserted into the call on behalf of the endpoint. MTP resource use remains invisible to both the users of the system and to the
endpoint on whose behalf it was inserted. If an MTP resource is not available when it is needed, the call connects without using an MTP resource, and that call does not have supplementary services.

Make sure that the Cisco IP Voice Media Streaming application is activated and running on the server on which the MTP device is configured.

The Cisco IP Voice Media Streaming application, which is common to the MTP, Conference Bridge, annunciator, and Music On Hold applications, runs as a service of Cisco Unified Communications Manager.

You can add an MTP device in two ways:

- You automatically add an MTP device when you activate the Cisco IP Voice Media Streaming Application service from Cisco Unified Serviceability.

- You can manually install the Cisco IP Voice Media Streaming Application on a networked server and configure an MTP device on that server through Cisco Unified Communications Manager Administration.

Manage MTPs with the Media Resource Manager

The Media Resource Manager (MRM), a software component in the Cisco Unified Communications Manager system, primarily functions for resource registration and resource reservation. Each MTP device that is defined in the database registers with the MRM. The MRM keeps track of the total available MTP devices in the system and of which devices have available resources.

During resource reservation, the MRM determines the number of resources, identifies the media resource type (in this case, the MTP), and the location of the registered MTP device.

The MRM updates its shared resource table with the registration information.

MRM also supports the coexistence of an MTP and transcoder within a Cisco Unified Communications Manager.

MTPs and Call Throttling

The MTP and Transcoder Resource Throttling Percentage service parameter, which supports the Cisco CallManager service, defines a percentage of the configured number of MTP or transcoder resources and allows Cisco Unified Communications Manager to extend the call to an MTP/transcoder that offers the best chance of successfully connecting the call. When the number of active MTP or transcoder resources is equal to or greater than the percentage that is configured for this parameter, Cisco Unified Communications Manager throttles (stops sending) calls to this MTP/transcoder. Cisco Unified Communications Manager hunts through the Media Resource Group List (MRGL) one time to find a MTP/transcoder that uses matching codecs on both sides of the call. If Cisco Unified Communications Manager cannot find an available MTP/transcoder with matching codecs, Cisco Unified Communications Manager returns to the top of the MRGL to repeat the search, which then includes those MTPs/transcoders that are in a throttled state and that match a smaller subset of capabilities for the call. Cisco Unified Communications Manager extends the call to the MTP/transcoder that is the best match for the call when Cisco Unified Communications Manager determines that a resource may be available; the call fails when the MTP/transcoder cannot allocate a resource for the call. In some cases, Cisco Unified Communications Manager perceives that a resource on a hardware MTP/transcoder is available, but the actual port on the hardware is not available.

For example, if you enter 40 for the Call Count service parameter, which supports the Cisco IP Voice Media Streaming Application service, for a software MTP or transcoder (or for hardware resources, if the maximum sessions is configured at 40, for example), and you set the MTP and Transcoder Resource Throttling Percentage service parameter to 95 percent, Cisco Unified Communications Manager throttles calls to the MTP/transcoder.
when 38 resources are used on this MTP/transcoder \((.95 \times 40 = 38)\). When a new request for an MTP or transcoder arrives, Cisco Unified Communications Manager checks whether the number of resources has dropped to 38 or less, and if so, extends the call to the MTP/transcoder.

For the maximum, minimum, and default values for this service parameter, click the question mark help in the Service Parameter Configuration window in Cisco Unified Communications Manager Administration.

### MTP types in Cisco Unified Communications Manager administration

The media termination point types in Cisco Unified Communications Manager Administration are as follows.

**Table 27: Media Termination Point Types**

<table>
<thead>
<tr>
<th>MTP Type</th>
<th>Description</th>
</tr>
</thead>
</table>
| Cisco IOS Enhanced Media Termination Point   | This type supports Cisco 2600XM, Cisco 2691, Cisco 3725, Cisco 3745, and Cisco 3660 Access Routers and the following MTP cases:  
  - For software-only implementation that does not use DSP but has the same packetization time for devices that support G.711 to G.711 or G.729 to G.729 codecs, this implementation can support up to 500 sessions per gateway.  
  - For a hardware-only implementation with DSP for devices that use G.711, G.729a, and G.729b codecs, 200 sessions can occur per NM-HDV2, and 48 sessions can occur per NM-HD.  
  Note: For more information on using G.729 codecs over SIP trunks, see [Session Initiation Protocol](#), on page 397  
  This type can support Network Address Translation in a service provider environment to hide the private address.  
  In Cisco Unified Communications Manager Administration, ensure that you enter the same MTP name that exists in the gateway Command Line Interface (CLI). |
| Cisco Media Termination Point Software       | A single MTP provides a default of 48 MTP (user configurable) resources, depending on the speed of the network and the network interface card (NIC). For example, a 100-MB Network/NIC card can support 48 MTP resources, while a 10-MB NIC card cannot.  
  For a 10-MB Network/NIC card, approximately 24 MTP resources can be provided; however, the exact number of MTP resources that are available depends on the resources that other applications on that PC are consuming, the speed of the processor, network loading, and various other factors. |

### Plan software MTP

Provisioning represents a crucial aspect that needs consideration when MTP resources are deployed. Provisioning requires attentive analysis of the call load patterns and the network topology.
Consider the following information when you are planning your MTP configuration:

- An improper setting can result in undesirable performance if the workload is too high.
- A single MTP provides a default of 48 MTP (user configurable) streams, and two streams make one resource because you need one stream for each side (send/receive) of the MTP. For a 10-MB Network/NIC card, approximately 24 MTP resources can be provided; however, the exact number of MTP resources that are available depends on the resources that other applications on that PC are consuming, the speed of the processor, network loading, and various other factors.

Consider the following formula to determine the approximate number of MTPs that are needed for your system, assuming that your server can handle 48 MTP streams (you can substitute 48 for the correct number of MTP resources that your system supports):

\[ \text{Number divided by 48} = \text{number of MTP applicationsthatare needed} \ (n/48 = \text{number of MTP applications}) \]

where:

- \( n \) represents the number of devices that require MTP support for H.323 and SIP calls.

If a remainder exists, add another server with Cisco IP Voice Streaming Application service with MTP.

- If one H.323 or SIP endpoint requires an MTP, it consumes one MTP resource. Depending on the originating and terminating device type, a given call might consume more than one MTP resource. The MTP resources that are assigned to the call get released when the call terminates.

- Use the Serviceability Real-Time Monitoring Tool (RTMT) to monitor the usage of MTP resources. The perfmon counter, Media TermPoints Out of Resources, increments for each H.323 or SIP call that connects without an MTP resource when one was required. This number can assist you in determining how many MTP resources are required for your callers and whether you have adequate coverage.

- Identical system requirements apply for the Cisco IP Voice Media Streaming Application, the MTP resources, and the Cisco Unified Communications Manager system.

- To optimize performance of DTMF signaling, use Cisco IOS release 12.4(11)T or later. This Cisco IOS release supports RFC 2833 DTMF MTP Passsthrough of digits.

**Software MTP device characteristics**

The Full Streaming Endpoint Duplex Count, a number of MTP resources that a specific MTP supports, represents a device characteristic that is specific to MTP device configuration.

**Avoid call failure**

To prevent call failure or user alert, avoid the following conditions:

- Although the Cisco IP Voice Media Streaming Application service can run on the same PC as the Cisco Unified Communications Manager, Cisco strongly recommends against this arrangement. If the Cisco IP Voice Media Streaming Application is running on the same PC as the Cisco Unified Communications Manager, it can adversely affect the performance of the Cisco Unified Communications Manager.

- When you configure the MTP, a prompt asks you to reset MTP before any changes can take effect. This action does not result in disconnection of any calls that are connected to MTP resources. If you choose **Reset**, as soon as the MTP has no active calls, the changes take effect.
When you make updates to the MTP and you choose Restart, all calls that are connected to the MTP get dropped.

**MTP system requirements and limitations**

The following system requirements and limitations apply to software MTP devices:

- You can activate only one Cisco IP Voice Streaming Application per server. To provide more MTP resources, you can activate the Cisco IP Voice Streaming application on additional networked servers.
- Each MTP can register with only one Cisco Unified Communications Manager at a time. The system may have multiple MTPs, each of which may be registered to one Cisco Unified Communications Manager, depending on how your system is configured.
- Cisco strongly recommends that you do not activate the Cisco IP Voice Streaming Media Application on a Cisco Unified Communications Manager with a high call-processing load because it can adversely affect the performance of the Cisco Unified Communications Manager.

**MTP failover and fallback**

This section describes how MTP devices failover and fallback when the Cisco Unified Communications Manager to which they are registered becomes unreachable. This section also explains conditions that can affect calls that are associated with an MTP device, such as MTP reset or restart.

**Active Cisco Unified Communications Manager becomes inactive**

The following description gives the MTP device recovery methods when the MTP is registered to a Cisco Unified Communications Manager that goes inactive:

- If the primary Cisco Unified Communications Manager fails, the MTP attempts to register with the next available Cisco Unified Communications Manager in the Cisco Unified Communications Manager Group that is specified for the device pool to which the MTP belongs.
- The MTP device reregisters with the primary Cisco Unified Communications Manager as soon as it becomes available after a failure and is currently not in use.
- The system maintains the calls or conferences that were active in call preservation mode until all parties disconnect. The system does not make supplementary services available.
- If an MTP attempts to register with a new Cisco Unified Communications Manager and the register acknowledgment is never received, the MTP registers with the next Cisco Unified Communications Manager.

**Reset registered MTP devices**

The MTP devices will unregister and then disconnect after a hard or soft reset. After the reset completes, the devices reregister with the Cisco Unified Communications Manager.
Dependency records

To find what media resource groups a specific media termination point is using, choose Dependency Records from the drop-down list box and click Go from the Cisco Unified Communications Manager Administration Media Termination Point Configuration window. The Dependency Records Summary window displays information about media resource groups that are using the media termination point. To find out more information about the media resource group, click the media resource group, and the Dependency Records Details window displays. If the dependency records are not enabled for the system, the dependency records summary window displays a message.

Software MTP performance monitoring and troubleshooting

The Real-Time Monitoring Tool counters for media termination point allow you to monitor the number of media termination points that are currently in use, the number of media termination points that are currently registered with Cisco Unified Communications Manager but are not currently in use, and the number of times that a media termination point was requested for a call, but no resources were available.

Cisco Unified Communications Manager writes all errors for the media termination point to the Local SysLog. In Cisco Unified Serviceability, you can set traces for the Cisco IP Voice Media Streaming Application service; to troubleshoot most issues, you must choose the Significant or Detailed option for the service, not the Error option. After you troubleshoot the issue, change the Debug Trace Level back to the Error option.

Cisco Unified Communications Manager generates registration and connection alarms for media termination point in Cisco Unified Serviceability.

If you need technical assistance, locate and review software MTP logs before you contact your Cisco Unified Communications partner or the Cisco Technical Assistance Center (TAC).

Use the following CLI commands to access the software MTP logs:

file list activelog cm/trace/cms/sdi/*.txt
file get activelog cm/trace/cms/sdi/*.txt
file view activelog cm/trace/cms/sdi/cms00000000.txt
file tail activelog cm/trace/cms/sdi/cms00000000.txt
This chapter provides information about how Cisco digital signal processor (DSP) resources are used for transcoding and conferencing. The modules, which are available for use with Cisco Unified Communications Manager, can perform conferencing, Media Termination Point (MTP), and transcoding services in addition to serving as a PSTN gateway.

- **Cisco DSP resources**, page 303
- **Supported Cisco Catalyst gateways and Cisco Access routers**, page 307

### Cisco DSP resources

DSP resources on the Cisco gateway, for example, Catalyst 4000 (WS-X4604-GWY), Catalyst 6000 (WS-6608-T1 or WS-6608-E1), Cisco 2600, Cisco 2600XM, Cisco 2800, Cisco 3600, Cisco 3700, Cisco 3800, or Cisco VG200, provide hardware support for IP telephony features that are offered by Cisco Unified Communications Manager. These features include hardware-enabled voice conferencing, hardware-based MTP support for supplementary services, and transcoding services.

**Note**

Verify with your Cisco account manager the devices that support conferencing, media termination points, and transcoding services.

The DSP resource management (DSPRM) maintains the state for each DSP channel and the DSP. DSPRM maintains a resource table for each DSP. The following responsibilities belong to DSPRM:

- Discover the on-board DSP SIMM modules and, based on the user configuration, determine the type of application image that a DSP uses.
- Reset DSPs, bring up DSPs, and download application images to DSP.
- Maintain the DSP initialization states and the resource states and manage the DSP resources (allocation, deallocation, and error handling of all DSP channels for transcoding and conferencing).
- Interface with the backplane Protocol Control Information (PCI) driver for sending and receiving DSP control messages.
• Handle failure cases, such as DSP crashes and session terminations.

• Provide a keepalive mechanism between the DSPs and the primary and backup Cisco Unified Communications Managers. The primary Cisco Unified Communications Manager can use this keepalive to determine when DSPs are no longer available.

• Perform periodic DSP resource checks.

When a request is received from the signaling layers for a session, the system assigns the first available DSP from the respective pool (transcoding or conferencing), as determined by media resource groups and media resource group lists, along with the first available channel. DSPRM maintains a set of MAX limits (such as maximum conference sessions per DSP or maximum transcoding session per DSP) for each DSP.

A switchover occurs when a higher order Cisco Unified Communications Manager becomes inactive or when the communication link between the DSPs and the higher order Cisco Unified Communications Manager disconnects. A switchback occurs when the higher order Cisco Unified Communications Manager becomes active again and DSPs can switch back to the higher order Cisco Unified Communications Manager. During a switchover and switchback, the gateway preserves active calls. When the call ends, the gateway detects RTP inactivity, DSP resources release, and updates occur on the Cisco Unified Communications Manager.

**Hardware-based MTP transcoding services**

Introducing the WAN into an IP telephony implementation forces the issue of voice compression. After a WAN-enabled network is implemented, voice compression between sites represents the recommended design choice to save WAN bandwidth. This choice presents the question of how WAN users use the conferencing services or IP-enabled applications, which support only G.711 voice connections. Using hardware-based MediaTerminationPoint (MTP)/transcoding services to convert the compressed voice streams into G.711 provides the solution.

The MTP service can act either like the original software MTP resource or as a transcoding MTP resource. An MTP service can provide supplementary services such as hold, transfer, and conferencing when the service is using gateways and clients that do not support the H.323v2 feature of EmptyCapabilitiesSet. The MTP, provided by the Cisco IP Voice Media Streaming Application service, can be activated as co-resident with Cisco Unified Communications Manager or activated separately without Cisco Unified Communications Manager. Both of these services operate on the Cisco Unified Communications Manager appliance (server). The Cisco IP Voice Media Streaming Application service installs as a component with Cisco Unified Communications Manager; however, for a dedicated MTP server, the Cisco CallManager service would not be activated (only the Cisco Voice IP Voice Media Streaming Application service).

When MTP is running in software on Cisco Unified Communications Manager, the resource supports 48 MTP sessions. When MTP is running on a separate Cisco Unified Communications Manager appliance (server), the resource supports up to 128 MTP sessions. In addition, Cisco Voice Gateway Routers also can provide MTP services.

Observe the following design capabilities and requirements for MTP transcoding:

• Provision MTP transcoding resources appropriately for the number of IP WAN callers to G.711 endpoints.

• Each transcoder has its own jitter buffer of 20-40 ms.

The following summary gives caveats that apply to MTP transcoding:

• Make sure that each Cisco Unified Communications Manager has its own configured MTP transcoding resource.
• If all n MTP transcoding sessions are utilized, and an n + 1 connection is attempted, the next call will complete without using the MTP transcoding resource. If this call attempted to use the software MTP function to provide supplementary services, the call would connect, but any attempt to use supplementary services would fail and could result in call disconnection. If the call attempted to use the transcoding features, the call would connect directly, but no audio would be received. If a transcoder is required but not available, the call would not connect.

For specific information on the number of sessions that are supported, see the Supported Cisco Catalyst gateways and Cisco Access routers, on page 307.

**IP-to-IP packet transcoding and voice compression**

You can configure voice compression between IP phones through the use of regions and locations in Cisco Unified Communications Manager. However, the Cisco Catalyst conferencing services and some applications currently support only G.711, or uncompressed, connections. For these situations, MTP transcoding or packet-to-packet gateway functionality provides modules for the Cisco Catalyst 4000 and Cisco Catalyst 6000. A packet-to-packet gateway designates a device with DSPs that has the job of transcoding between voice streams by using different compression algorithms. For example, a user on an IP phone at a remote location calls a user at the central location. Cisco Unified Communications Manager instructs the remote IP phone to use compressed voice, or G.729a, only for the WAN call. If the called party at the central site is unavailable, the call may roll to an application that supports G.711 only. In this case, a packet-to-packet gateway transcodes the G.729a voice stream to G.711 to leave a message with the voice-messaging server.

**Voice compression IP-to-IP packet transcoding and conferencing**

Connecting sites across an IP WAN for conference calls presents a complex scenario. In this scenario, the modules must perform the conferencing service as well as the IP-to-IP transcoding service to uncompress the WAN IP voice connection. In the figure below, a remote user joins a conference call at the central location. This three-participant conference call uses seven DSP channels on the Catalyst 4000 module and three DSP channels on the Cisco Catalyst 6000. The following list gives the channel usage:

• Cisco Catalyst 4000
  - One DSP channel to convert the IP WAN G.729a voice call into G.711
  - Three conferencing DSP channels to convert the G.711 streams into TDM for the summing DSP
  - Three channels from the summing DSP to mix the three callers together

• Cisco Catalyst 6000
Three conferencing DSP channels. On the Cisco Catalyst 6000, all voice streams get sent to single logical conferencing port where all transcoding and summing takes place.

**Figure 33: Multisite WAN Using Centralized MTP Transcoding and Conferencing Services**

**IP-to-IP packet transcoding across intercluster trunks**

Intercluster trunks connect Cisco Unified Communications Manager clusters. Intercluster trunks allocate a transcoder on a dynamic basis.

The Cisco Catalyst 6000 module uses the MTP service regardless of whether transcoding is needed for a particular intercluster call. Cisco Unified Communications Manager supports compressed voice call connection through the MTP service if a hardware MTP is used.

The following list gives intercluster MTP/transcoding details:

- Outbound intercluster calls will use an MTP/transcoding resource from the Cisco Unified Communications Manager from which the call originates.
- Inbound intercluster call will use the MTP/resource from the Cisco Unified Communications Manager that terminates the inbound intercluster trunk.
- Allocate additional DSP MTP/transcoding resources to Cisco Unified Communications Managers terminating intercluster trunks.
- For compressed callers, you can accurately provision the MTP transcoding resources.

**Hardware-based conferencing services**

Hardware-enabled conferencing designates the ability to support voice conferences by using DSPs to perform the mixing of voice streams to create multiparty conference sessions. The voice streams connect to conferences through packet or time-division-multiplexing (TDM) interfaces.
The network modules, depending on the type, support both uncompressed and compressed VOIP conference calls. The modules use Skinny Client Control Protocol to communicate with Cisco Unified Communications Manager to provide conferencing services. When the conferencing service registers with Cisco Unified Communications Manager, it announces that only G.711 calls can connect to the conference. If any compressed calls request to join a conference, Cisco Unified Communications Manager connects them to a transcoding port first to convert the compressed call to G.711.

Observe the following recommendations when you are configuring conferencing services:

- When you are provisioning an enterprise with conference ports, first determine how many callers will attempt to join the conference calls from a compressed Cisco Unified Communications Manager region. After you know the number of compressed callers, you can accurately provision the MTP transcoding resources.

- Conference bridges can register with more than one Cisco Unified Communications Manager at a time, and Cisco Unified Communications Managers can share DSP resources through the Media Resource Manager (MRM).

For specific information on the number of sessions that are supported, see the Supported Cisco Catalyst gateways and Cisco Access routers, on page 307.

**Supported Cisco Catalyst gateways and Cisco Access routers**

The following section provides specific information on the number of supported conferencing, transcoding, and MTP sessions for Cisco Catalyst Gateways and Cisco Access Routers.

**Cisco Catalyst 4000 WS-X4604-GWY**

The PSTN gateway and voice services module for the Cisco Catalyst 4003 and 4006 switches supports three analog voice interface cards (VICs) with two ports each or one T1/E1 card with two ports and two analog VICs. Provisioning choices for the VIC interfaces include any combination of Foreign Exchange Office (FXO), Foreign Exchange Station (FXS), or Ear & Mouth (E&M). Additionally, when configured as an IP telephony gateway from the command-line interface (CLI), this module can support conferencing and transcoding services.

You can configure the Cisco Catalyst 4000 voice gateway module in either toll bypass mode or gateway mode; however, you can configure the module conferencing and transcoding resources only in gateway mode. Gateway mode designates the default configuration. From the CLI, you can change the conferencing-to-transcoding ratios. After the gateway mode is enabled, the 24 DSPs (4 SIMMs with 6 DSPs each) for the module occur as described in the following bullets:

- Over the PSTN gateway using G.711 only-96 calls
- In a G.711 conference only-24 conference participants; maximum of 4 conferences of 6 participants each

Unlike the WS-X6608-x1, which can mix all conference call participants, the Cisco Catalyst 4000 WS-X4604-GWY module sums only the three dominant speakers. The WS-X4604-GWY dynamically adjusts for the dominant speakers and determines dominance primarily by voice volume, not including any background noise.
The Cisco Catalyst 4000 conferencing services support G.711 connections only, unless an MTP transcoding service is used.

Caution

- Transcoding to G.711-16 MTP transcoding sessions

The following information applies to the Cisco Catalyst 4000 module:

- The WS-X4604-GWY uses a Cisco IOS interface for initial device configuration. All additional configuration for voice features takes place in Cisco Unified Communications Manager.

- The WS-X4604-GWY can operate as a PSTN gateway (toll bypass mode) as well as a hardware-based transcoder or conference bridge (gateway mode). To configure this module as a DSP farm (gateway mode), enter one or both of the following CLI commands:

  ```
  voicecard conference
  voicecard transcode
  ```

- The WS-X4604-GWY requires its own local IP address in addition to the IP address for Cisco Unified Communications Manager. Specify a loopback IP address for the local Signaling Connection Control Part.

- You can define a primary, secondary, and tertiary Cisco Unified Communications Manager for both the conferencing and MTP transcoding services.

Cisco Catalyst 6000 WS-6608-T1 or WS-6608-E1

The WS-6608-T1 (or WS-6608-E1 for European countries) designates the same module that provides T1 or E1 PSTN gateway support for the Cisco Catalyst 6000. This module comprises eight channel-associated-signaling (CAS) or primary rate interface (PRI) interfaces, each of which has its own CPU and DSPs. After the card is added from Cisco Unified Communications Manager as a voice gateway, you configure it as a conferencing or MTP transcoding resource. Each port acts independently of the other ports on the module. Specifically, you can configure each port only as a PSTN gateway interface, a conferencing node, or an MTP transcoding node. In most configurations, configure a transcoding resource for each conferencing resource.

Whether acting as a PSTN gateway, a conferencing resource, or an MTP transcoding resource, each port on the module requires its own IP address. Configure the port to have either a static IP address or an IP address that the DHCP provides. If a static IP is entered, you must also add a TFTP server address because the ports actually get all configuration information from the downloaded TFTP configuration file.
The following figure shows one possible configuration of the Cisco Catalyst 6000 voice gateway module. This diagram shows two of the eight ports of the module as configured in PSTN gateway mode, three ports in conferencing mode, and three ports in MTP transcoding mode.

**Figure 34: Cisco Catalyst 6000 Voice Gateway Module**

After a port is configured through the Cisco Unified Communications Manager interface, each port can support one of the following configurations:

- WS-6608-T1 over the PSTN gateway - 24 calls per physical DS1 port; 192 calls per module
- WS-6608-E1 over the PSTN gateway - 30 calls per physical DS1 port; 240 calls per module
- For a G.711 or G.723 conference - 32 conferencing participants per physical port; maximum conference size of 16 participants
- For a G.729 conference - 24 conferencing participants per physical port; maximum conference size of 16 participants

**Tip**

After the WS-X6608 is added as a T1 or E1 Cisco gateway, you can configure it, on a per-port basis, for conferencing services.

On the Cisco Catalyst 6000, conferencing services cannot cross port boundaries.

The following capacities apply to simultaneous transcoding and conferencing:

- For transcoding from G.723 to G.711 - 32 MTP transcoding sessions per physical port; 256 sessions per module
- For transcoding from G.729 to G.711 - 24 MTP transcoding sessions per physical port; 192 sessions per module

**Cisco 2600 Cisco 2600XM Cisco 2800 Cisco 3600 Cisco 3700 Cisco 3800 and Cisco VG200 for NM-HDV**

NM-HDV supports the previous Cisco gateways.

The following list represents the maximum number of sessions:
• G.711, G.729, GSM FR, and GSM EFR conference sessions-Per network module, 15

Tip
Maximum participants per conference session equals 6.

• Transcoding from G.711 to G.729-Per network module, 60
• Transcoding from G.711 to GSM FR/GSM EFR-Per network module, 45

Caution
On these gateways, transcoding services cannot cross port boundaries.
Cisco MTP transcoding service only supports HBR codec to G.711 conversion and vice versa. No support exists for LBR-to-LBR codec conversion.

Cisco 2600XM Cisco 2691 Cisco 2800 Cisco 3600 Cisco 3700 and Cisco 3800 for NM-HD and NM-HDV2

Tip
The NM-HDV2 does not support the Cisco 3660.

The following list represents the maximum number of sessions that are available for conferences, transcoding, and MTP for NM-HD and NM-HDV2:

Per NM-HD-1V/2V
• G.711 only conference-8 sessions
• G.729, G.729a, G.729ab, and G.729b conference-2 sessions
• GSM FR conference-Not applicable
• GSM EFR conference-Not applicable

Tip
Maximum number of participants per conference equals 8.

• Transcoding for G.711 to G.729a/G.729ab/GSMFR-8 sessions
• Transcoding for G.711 to G.729/G.729b/GSM EFR-6 sessions

Per NM-HDV2
• G.711 only conference-50 sessions
• G.729, G.729a, G.729ab, G.729b conference-32 sessions
• GSM FR conference-14 sessions
• GSM EFR conference-10 sessions
• Transcoding for G.711 to G.729a/G.729ab/GSMFR-128 sessions
• Transcoding for G.711 to G.729/G.729b/GSM EFR-96 sessions

For a software MTP (DSP-less with same packetization period for both devices supporting G.711 to G.711 or G.729 to G.729 codecs), 500 sessions can occur per gateway; for a hardware MTP (with DSP, using G.711 codec only), 200 sessions can occur per NM-HDV2 and 48 per NM-HD.

**Tip**

Maximum number of participants per conference equals 8.
Supported Cisco Catalyst gateways and Cisco Access routers
PART VI

Voice Mail and messaging integration

- Voice Mail connectivity to Cisco Unified Communications Manager, page 315
- SMDI Voice Mail integration, page 325
- Cisco Unity Messaging integration, page 331
- Cisco DPA integration, page 335
This chapter provides information about the voice-messaging system, which is an integral part of an enterprise telecommunications system, provides voice-messaging features for all users. After receiving voice messages in their mailboxes, users receive message-waiting lights on their phones. Users can retrieve, listen to, reply to, forward, and delete their messages by accessing the voice-messaging system with an internal or external call.

You must enter all users and their directory numbers in Cisco Unified Communications Manager Administration to make it possible for them to retrieve messages from a Cisco Unity voice-mail device.

Cisco Unified Communications Manager supports an increasing variety of voice-messaging systems and provides configuration of message-waiting indicators for all users, including those with shared line appearances.

As the size or number of Cisco Unified Communications Manager clusters increases in an enterprise, the likelihood that an administrator needs to deploy multiple voice-messaging systems also increases.

- Voice Mail interfaces, page 315
- Voice Mail system access, page 316
- Message Waiting, page 318
- Prime line support for voice messaging, page 319
- Call Forwarding in a multiple Voice Mail system environment, page 321
- Call Transfer with voice messaging systems, page 322

Voice Mail interfaces

Cisco Unified Communications Manager supports both directly connected and gateway-based messaging systems. Directly connected voice-messaging systems communicate directly with Cisco Unified Communications Manager by using a packet protocol. A gateway-based voice-messaging system connects to Cisco Unified Communications Manager through analog or digital trunks that connect to Cisco gateways.
Cisco Unified Communications Manager interacts with voice-messaging systems by using the following types of interfaces:

- **Skinny Protocol**—Directly connected voice-messaging systems that use Skinny protocol could use other protocols to communicate with Cisco Unified Communications Manager. In Cisco Unified Communications Manager Administration, you configure the interface to directly connected voice-messaging systems by creating voice-mail ports. To handle multiple, simultaneous calls to a voice-messaging system, you create multiple voice-mail ports and place the ports in a line group and the line group in a route/hunt list. Directly connected voice-messaging systems send message-waiting indications by calling a message-waiting on and off number that is configured in Cisco Unified Communications Manager Administration.

When you configure security for voice-mail ports and Cisco Unity SCCP devices, a TLS connection (handshake) opens for authenticated devices after each device accepts the certificate of the other device; likewise, the system sends SRTP streams between devices; that is, if you configure the devices for encryption.

When the device security mode equals authenticated or encrypted, the Cisco Unity TSP connects to Cisco Unified Communications Manager through the Cisco Unified Communications Manager TLS port. When the security mode equals nonsecure, the Cisco Unity TSP connects to Cisco Unified Communications Manager through the Cisco Unified Communications Manager SCCP port.

- **PSTN Gateway Interfaces**—H.323-based voice-messaging systems and legacy voice-messaging systems use PSTN gateway interfaces. These systems usually (but not necessarily) send message-waiting indications by using Simplified Message Desk Interface (SMDI) over an EIA/TIA-232 interface. Cisco Unified Communications Manager also sends call history messages to the voice-messaging system by using this same SMDI interface. The Cisco Messaging Interface service relays these indications to Cisco Unified Communications Manager. In Cisco Unified Communications Manager Administration, you can provision the interface to gateway-based voice-messaging systems simply by provisioning an analog FXS gateway or a digital T1/E1 gateway with CAS or PRI protocols. By creating a route group that contains individual gateway ports or T1 spans, you can enable simultaneous calls to a voice-messaging system. In addition, if the voice-messaging system user SMDI, you must configure and run the Cisco Messaging Interface service.

- **Intercluster Interfaces**—A Cisco Unified Communications Manager in one cluster can provide access to a voice-messaging system in another cluster, if the administrator provisions the voice-mail pilot number on the intercluster trunk. Voice-messaging systems can leave messages and set message-waiting indicators for devices in other clusters if the clusters are connected by QSIG trunks.

### Voice Mail system access

For directly connected voice-messaging systems, Cisco Unified Communications Manager uses directory numbers that are assigned to voice-mail ports. Administrators assign the voice-mail ports to a line group and place the line group in a route/hunt list. If multiple users attempt to access a voice-messaging system at the same time, all users have an available port for access to the voice-messaging system. When users access their voice messages, they dial the voice-mail pilot number or press the messages button on the phone.

For gateway-based voice-messaging systems, Cisco Unified Communications Manager uses route lists. When a user calls the route list number, the route list offers incoming calls to each port of the voice-messaging system by using a search algorithm. For gateway-based voice-messaging systems, the voice-mail pilot number specifies the route list itself.
Calls to directory numbers that are associated with voice-messaging systems cause the called voice-messaging systems to handle the call. When calls are made directly to voice-messaging systems, the system prompts the user for mailbox and password information for message retrieval.

Users can reach a voice-messaging system either by entering the voice-mail pilot number, if known, or by pressing the messages button on a Cisco Unified IP Phone in the 7900 series. When a user presses the messages button, a call goes to the voice-mail pilot number that the administrator has configured for the line that is currently in use on the Cisco Unified IP Phone. When no voice-mail pilot number is configured for the active line, Cisco Unified Communications Manager directs voice-messaging calls to a default profile.

**Voice Mail pilot numbers**

The voice-mail pilot number specifies the directory number that you dial to access your voice messages. Cisco Unified Communications Manager automatically dials the voice-messaging number when you press the messages button on your phone. Each voice-mail pilot number can belong to a different voice-messaging system.

The Voice Mail Pilot Configuration window of Cisco Unified Communications Manager Administration defines the voice-messaging number.

A default voice-mail pilot number exists in Cisco Unified Communications Manager. You can create a new default voice-mail pilot number that replaces the current default setting.

**Voice Mail profiles**

Different lines on a device can have different voice-mail profiles. For example, an administrative assistant phone can have a second line for the manager, which routes to the manager voice-messaging system. The administrative assistant line routes to its own voice-messaging system.

Voice-mail profiles allow you to define any line-related, voice-mail information that is associated to a directory number, not a device. The voice-mail profile contains the following information:

- Voice Mail Profile Name
- Description
- Voice Mail Pilot Number
- Voice Mail Box Mask
- Default (checked if this particular profile is the default profile)

A predefined, default voice-mail profile automatically gets assigned to lines when the administrator adds a line. When you search for voice-mail profiles, “default” appears beside the profile name within the list.

A voice-mail profile takes precedence over other settings when calls are routed to a voice-messaging system.

**Tip**

When a call gets redirected from a DN to a voice-messaging server/service that is integrated with Cisco Unified Communications Manager by using a SIP trunk, the voice mailbox mask on the voice-mail profile for the phone modifies the diverting number in the SIP diversion header. Be aware that this behavior is expected because Cisco Unified Communications Manager uses the diversion header to choose a mailbox.
Message Waiting

For directly connected voice-messaging systems, you can configure message waiting by using a single configuration window in Cisco Unified Communications Manager Administration. The Message Waiting Configuration window defines directory numbers for message-waiting on and message-waiting off indicator. A directly connected voice-messaging system uses the specified directory number to set or to clear a message-waiting indication for a particular Cisco Unified IP Phone.

The Message Waiting Configuration window of Cisco Unified Communications Manager Administration provides for the following information:

- Confirmation of multiple message-waiting on and off numbers for a Cisco Unified Communications Manager cluster.
- Explicit association of a message-waiting search space with each message-waiting on and off number
- Validation of the message-waiting number and calling search space entry
- Search for conflicting numbers in the numbering plan.

Message Waiting indication

When a caller leaves a message in a mailbox, the voice-messaging system sends a message-waiting indication to the party that received the voice message. Similarly, when the owner of a voice mailbox deletes all pending voice messages, the voice-messaging system sends a message-waiting indication off to inform the voice-mailbox owner that no more messages are pending.

Cisco Unified Communications Manager enables administrators to configure how to turn on the handset indicator of Cisco Unified IP Phones 7940 and 7960 for pending voice messages. You can configure Cisco Unified Communications Manager to do one of the following actions:

- Light the message-waiting lamp and display the prompt if a message is waiting on primary line.
- Display the prompt if a message is waiting on primary line.
- Light the message-waiting lamp if a message is waiting on primary line.
- Light the message-waiting lamp and display the prompt if a message is waiting on any line.
- Display only the prompt, if a message is waiting on any line.
- Display only the message-waiting lamp, if a message is waiting on any line.
- Do not light the message-waiting lamp or display the prompt.

You can set the message-waiting indication policy by using two different methods:

- Directory Number Configuration-Use the Message Waiting Lamp Policy field to set when the handset lamp turns on for a given line. Use the following available settings:
  - Use System Policy
  - Light and Prompt
  - Prompt Only
  - Light Only
• None

• Service Parameter Configuration (for the Cisco CallManager service)-Use the Message Waiting Lamp Policy clusterwide service parameter to set the message-waiting indication policy for all Cisco Unified IP Phones of the 7900 series. Use the following available settings:

  ◦ Primary Line - Light and Prompt
  ◦ Primary Line - Prompt Only
  ◦ Primary Line - Light Only
  ◦ Light and Prompt
  ◦ Prompt Only
  ◦ Light Only
  ◦ None

The message-waiting policy that you choose depends on the needs of your users. For example, an administrative assistant, who shares the manager directory number as a secondary directory number, may want to have the policy set to Light and Prompt. The administrator can see whether the manager line has pending voice messages. General office members, who share a line appearance with a coworker, might set the policy so the indicator lights only when messages are pending for the primary line appearance.

For customers who do not have complex message-waiting indicator requirements, you can use the Cisco CallManager service parameter to dictate the conditions under which Cisco Unified Communications Manager turns on the message-waiting lamp.

Tip
The Multiple Tenant MWI Modes service parameter, which supports the Cisco CallManager service, specifies whether to apply translation patterns to voice-message mailbox numbers. Valid values specify True, which means that Cisco Unified Communications Manager uses translation patterns to convert voice-message mailbox numbers into directory numbers when your voice-messaging system issues a command to set a message waiting indicator, or False, which means that Cisco Unified Communications Manager does not translate the voice-message mailbox numbers that it receives from your voice-messaging system. Be aware that this service parameter supports Cisco Unified Communications Manager integrations with Cisco Unity Connection. If your voice-mail extensions require translation in Cisco Unified Communications Manager, set the Multiple Tenant MWI Modes service parameter to True after you install or upgrade to Cisco Unified Communications Manager 8.5(1).

Prime line support for voice messaging

With prime line support for voice messaging, the primary line on the phone always becomes the active line for retrieving voice messages when the phone user presses the Messages button on the phone.

You can configure the Always Use Prime Line for Voice Mail service parameter for the Cisco CallManager service or you can configure the Always Use Prime Line for Voice Message setting for devices and device profiles. The Always Use Prime Line for Voice Message setting displays in the following windows in Cisco Unified Communications Manager Administration.

• System > Service Parameters (for Cisco CallManager service)
For information on how the Always Use Prime Line for Voice Messages setting works when a phone idle or busy, see Table 29-1 on page 29-6.

---

**Tip**

If you configure the Always Use Prime Line for Voice Message setting in the Service Parameter, Common Phone Profile, and in the Phone Configuration window, Cisco Unified Communications Manager uses the configuration from the Phone Configuration window.

---

### Table 28: Always Use Prime Line for Voice Mail Configuration

<table>
<thead>
<tr>
<th>State of Phone</th>
<th>Configuration for Always Use Prime Line for Voice Message</th>
<th>How Feature Works</th>
</tr>
</thead>
<tbody>
<tr>
<td>Idle</td>
<td>On</td>
<td>If the phone is idle, the primary line on the phone becomes the active line for retrieving voice messages when the phone user presses the Messages button on the phone. If you choose On for the Always Use Prime Line for Voice Mail setting in the Device Profile or Default Device Profile Configuration window, a Cisco Extension Mobility user can use this feature after logging in to the device that supports Cisco Extension Mobility; that is, if you configure Cisco Extension Mobility correctly.</td>
</tr>
<tr>
<td>Idle</td>
<td>Off</td>
<td>If the phone is idle, pressing the Messages button on the phone automatically dials the voice-messaging system from the line that has a voice message. It will always select the first line that has a voice message. If no line has a voice message, the primary line gets used when the phone user presses the Messages button.</td>
</tr>
<tr>
<td>Idle</td>
<td>Default</td>
<td>If you choose Default for the Always Use Prime Line for Voice Mail setting in the Phone Configuration, the Common Phone Profile, the Device Profile, or the Default Device Profile Configuration windows, Cisco Unified Communications Manager uses the configuration from the Always Use Prime Line service parameter when it determines whether a user, including a Cisco Extension Mobility user, can use this feature. If you choose Default for the Always Use Prime Line for Voice Mail setting in the Phone Configuration window, Cisco Unified Communications Manager uses the configuration from the common phone profile.</td>
</tr>
</tbody>
</table>
### How Feature Works

<table>
<thead>
<tr>
<th>State of Phone</th>
<th>Configuration for Always Use Prime Line for Voice Message</th>
<th>How Feature Works</th>
</tr>
</thead>
<tbody>
<tr>
<td>Busy</td>
<td>On</td>
<td>If the device is busy, this feature does not work.</td>
</tr>
</tbody>
</table>

**Tip**

Prime line support for voice messaging relies on the Cisco CallManager service, so activate the service by choosing **Tools > Service Activation** in Cisco Unified Serviceability. In addition, you can run SDI trace for the Cisco CallManager service. When you view the log in RTMT, you can see the configured value that the device uses; for example, `alwaysUsePrimeLineForVM=2`, which indicates that the device uses the default.

**Note**

If you want to do so, you can configure prime line support for voice messaging in the Bulk Administration Tool.

---

**Call Forwarding in a multiple Voice Mail system environment**

Voice-messaging systems support a maximum number of users just as Cisco Unified Communications Manager supports a maximum number of users.

To ensure that calls are forwarded to the voice-messaging system that is associated with the user for whom a voice message is intended, the Call Forward feature gets modified when calls are forwarded to voice-messaging systems.

Cisco Unified Communications Manager supports multiple voice-mail pilot numbers (profiles). Each pilot number can belong to a different voice-messaging system. Configure the voice-mail pilot profile on a line-by-line basis. Cisco Unified Communications Manager forwards a voice-mail call to the voice-messaging system of the original redirect endpoint (directory number) if it has the voice-mail pilot profile.

One limitation exists for intercluster call forwarding. When a call is forwarded from another cluster and then sent to voice-messaging system, Cisco Unified Communications Manager forwards the call to the voice-messaging system of the first redirect endpoint in the cluster. This occurs because Cisco Unified Communications Manager does not have the voice-mail pilot profile of the original endpoint in the other cluster. However, if a QSIG trunk links the clusters, the forwarded call will have the correct voice mailbox number but not the voice mail pilot number.

The Directory Number Configuration window of Cisco Unified Communications Manager Administration contains Call Forward and Call Pickup Settings. If the Voice Mail check box is chosen, Cisco Unified Communications Manager can Forward All, Forward Busy, or Forward No Answer to all devices for the chosen voice mail profile.
Examples

**Intracluster call-forwarding chains where the final forwarding phone has used the Forward To Voice Mail option**

A call forwards-all from a phone that is served by one voice-mail pilot to a phone that is served by another voice-mail pilot. The second phone forwards to voice mail. Cisco Unified Communications Manager delivers the call to the voice-mail pilot number that is associated with the first phone.

**Intracluster call-forwarding chains where the final forwarding phone has not used the Forward To Voice Mail option**

A call forward all from a phone that is served by one voice-mail pilot to a phone that is served by another voice-mail pilot. The second phone forwards to voice mail, but the voice-mail pilot number was entered as a specific numerical destination and not as a forward-to voice mail. Cisco Unified Communications Manager delivers the call to the voice-mail pilot number that is associated with the last phone.

**Intracluster call-forwarding chains with CTI**

When Cisco Unified Communications Manager Attendant Console or other CTI applications take control of a call, they often choose to eliminate information about the original call, so the next destination receives voice messages. Cisco Unified Communications Manager must direct the call to the voice-messaging system that manages the voice mailbox that Cisco Unified Communications Manager reports as the target voice mailbox, as shown in the following examples.

A call arrives at a phone, which forwards to the attendant console; the calling user dials by name, and Cisco Unified Communications Manager extends the call to a destination. The destination forwards to the voice-messaging system. Cisco Unified Communications Manager delivers the call to the voice-messaging number that is associated with the destination that the calling user chose, not the attendant console.

In another example, phone A forwards all calls to phone B. A call arrives at the attendant console, and the attendant console sends the call to phone A. Cisco Unified Communications Manager forwards the call to phone B. If no one answers the call, Cisco Unified Communications Manager forwards the call to the voice-messaging system. Because the call was originally for phone A, the message goes to the voice mailbox of phone A, not phone B.

**Intercluster call-forwarding chains**

In an intercluster call scenario, phone A on a Cisco Unified Communications Manager calls phone B on the same Cisco Unified Communications Manager. The call forwards over an intercluster trunk to Cisco Unified Communications Manager, which extends the call to phone C. Phone C forwards to the voice-messaging system. Cisco Unified Communications Manager extends the call to the voice-messaging system that is associated with phone C but reports the extension number of phone B.

No available voice-mail pilot number information exists about phone B because of the intercluster boundary. Therefore, Cisco Unified Communications Manager sends the call to the voice-mail pilot number that is associated with the final destination but reports the directory number that was passed from the PBX to Cisco Unified Communications Manager as the voice mailbox.

**Call Transfer with voice messaging systems**

Users, who have reached a voice-messaging system over a Catalyst 6000 FXS Analog Interface Module or a Cisco 6608 T1 CAS gateway, can transfer out of the voice-messaging system to another destination. By
responding to a voice-messaging prompt, the user enters a number. The voice-messaging system initiates the action by using a hookflash transfer. Cisco Unified Communications Manager responds by doing a blind transfer of the call to the target number. When the call transfer completes, the voice channel that connected the original call to the voice-messaging system gets released.

Configure hookflash detection timers for the Catalyst 6000 Voice T1 Voice Service Module by using Cisco Unified Communications Manager Administration Gateway Configuration.

![Note](image)

Only E&M T1 ports support the hookflash transfer.
SMDI Voice Mail integration

This chapter provides information about Simplified Message Desk Interface (SMDI) which defines a way for a phone system to provide voice-messaging systems with the information that the system needs to intelligently process incoming calls. Each time that the phone system routes a call, it sends an SMDI message through an EIA/TIA-232 connection to the voice-messaging system that tells it the line that it is using, the type of call that it is forwarding, and information about the source and destination of the call.

The SMDI-compliant voice-messaging system connects to Cisco Unified Communications Manager in two ways:

- Using a standard serial connection to the Cisco Unified Communications Manager
- Using POTS line connections to a Cisco analog FXS gateway

Configure SMDI

Simplified Message Desk Interface (SMDI) defines a way for a phone system to provide voice-messaging systems with the information that the system needs to intelligently process incoming calls. Each time that the phone system routes a call, it sends an SMDI message through an EIA/TIA-232 connection to the voice-messaging system that tells it the line that it is using, the type of call that it is forwarding, and information about the source and destination of the call.

The SMDI-compliant voice-messaging system connects to Cisco Unified Communications Manager in two ways:

- Using a standard serial connection to the Cisco Unified Communications Manager
- Using POTS line connections to a Cisco analog FXS gateway

An overview of the steps that are required to integrate voice-messaging systems that are using SMDI is as follows.
Procedure

Step 1  Add and configure gateway ports. If you are configuring an Octel system and you are using a Cisco Catalyst 6000 24 Port FXS Analog Interface Module or AST ports, make sure to set the Call Restart Timer field on each port to 1234.

Step 2  Create a route group and add the gateway ports that was configured to the route group.

Step 3  Create a route list that contains the route group that was configured.

Step 4  Create a route pattern.

Step 5  Activate, configure, and run the Cisco Messaging Interface service.

Step 6  Configure Cisco Messaging Interface trace parameters.

Step 7  Configure your voice-messaging system and connect the voice-messaging system to Cisco Unified Communications Manager with an EIA/TIA-232 cable. To connect the EIA/TIA-232 cable to Cisco Unified Communications Manager, use a Cisco certified serial-to-USB adapter.

SMDI voice messaging integration requirements

The Cisco Messaging Interface service allows you to use an external voice-messaging system with Cisco Communications Manager Release 3.0 and later.

The voice-messaging system must meet the following requirements:

- The voice-messaging system must have a simplified message desk interface (SMDI) that is accessible with a null-modem EIA/TIA-232 cable (and an available serial port). To connect the EIA/TIA-232 cable to Cisco Unified Communications Manager, use a Cisco-certified serial-to-USB adapter.

- The voice-messaging system must use analog ports for connecting voice lines.

- The Cisco Unified Communications Manager server must have an available serial or USB port for the SMDI connection.

- A Cisco Access Analog Station Gateway, Cisco Catalyst 6000 24-port FXS gateway, Cisco VG200 gateway, or Cisco Catalyst 6000 8-port T1 gateway that is configured with FXS ports must be installed and configured.

- You must ensure that gateways are configured in a route pattern.

Be aware that you must configure the following Cisco Messaging Interface service parameters per node if you use the CMI service to deploy multiple third-party voice-messaging systems in the same Cisco Unified Communications Manager cluster.

- CallManager Name
- Backup CallManager Name
- Voice Mail DN
- Voice Mail Partition
- Alternate DN
- Alternate DN Partition
After you configure these parameters in the Service Parameters Configuration window, a message displays that warns that you must configure the value on each node in the cluster to achieve clusterwide support.

**Configure port for SMDI**

Previous releases of Cisco Unified Communications Manager required a specific configuration for voice-messaging integration by using the SMDI and the Cisco Messaging Interface. This older configuration method for FXS ports required each individual port of an analog access gateway (Cisco AS-2, Cisco AS-4, Cisco AS-8, or Cisco Catalyst 6000 24 Port FXS gateway) to be explicitly configured as a separate entry in a route group. The relative position within the route list/route group of each analog access port determined the SMDI port number that the Cisco Messaging Interface reported.

For Cisco Communications Manager Release 3.0(5) and later releases, you can configure the SMDI port number through Cisco Unified Communications Manager Administration.

If you use the Cisco Catalyst 6000 8-port T1 gateway (6608) to interface with voice-messaging system, you must configure the SMDI base port for each T1 span.

To use the new SMDIPortNumber configuration, perform the following steps:

**Procedure**

**Step 1**
Modify each analog access port that connects to the voice-messaging system and set the SMDIPortNumber equal to the actual port number on the voice-messaging system to which the analog access port connects. With this first step, you do not need to change any route lists/route groups. The newly configured SMDIPortNumber(s) override any existing route list/route group configuration that was set up for the devices that connect to the voice-messaging system.

**Step 2**
To take advantage of reduced Cisco Unified Communications Manager signaling requirements with this new configuration, change each analog access device that is in a route group that was set up for the older method of configuration from multiple entries that identify individual ports on the device to a single entry in the route group that identifies “All Ports” as the port selection.

The selection order of each of these device entries differs or does not differ.

**Cisco Messaging Interface redundancy**

Most voice-messaging systems that rely on an EIA/TIA-232 serial cable (previously known as a RS-232 cable) to communicate with phone systems only have one serial port. You can achieve Cisco Messaging Interface redundancy by running two or more copies of the Cisco Messaging Interface service on different servers in a Cisco Unified Communications Manager cluster and using additional hardware including a data splitter that is described later in this section.

Each copy of Cisco Messaging Interface connects to a primary and backup Cisco Unified Communications Manager and registers to the Cisco Unified Communications Manager by using the same VoiceMailDn and VoiceMailPartition service parameter values. The Cisco Messaging Interface with the higher service priority (the active Cisco Messaging Interface service) handles the SMDI responsibilities. If this Cisco Messaging
Interface encounters problems, another one can take over. The figure below illustrates one of many layouts that provide Cisco Messaging Interface redundancy.

**Figure 35: Cisco Messaging Interface Redundancy**

To achieve Cisco Messaging Interface redundancy, you must have a device such as the data splitter as shown in the figure above to isolate the SMDI messaging from the various Cisco Messaging Interface services. You cannot use an ordinary Y-shaped serial cable to combine the EIA/TIA-232 streams together.

**Note**

To achieve Cisco Messaging Interface redundancy, you must have a device such as the data splitter as shown in the figure above to isolate the SMDI messaging from the various Cisco Messaging Interface services. You cannot use an ordinary Y-shaped serial cable to combine the EIA/TIA-232 streams together.

The data splitter that you connect to your voice-messaging system, such as the B&B Electronics modem data splitter (models 232MDS and 9PMDS), must have the following characteristics:

- High reliability
- Bidirectional communication
- Minimal transmission delay
- No external software support (desired)
- No extra EIA/TIA-232 control line operations (desired)

The 232MDS includes two DB25 male ports and one DB25 female port. The 9PMDS represents a DB9 version of this modem data splitter. These switches enable Cisco Messaging Interface redundancy with the following limitations when you set the ValidateDNs Cisco Messaging Interface service parameter to False:

- Two Cisco Messaging Interfaces cannot transmit SMDI messages simultaneously. Under extreme circumstances, you may experience network failures that break your Cisco Unified Communications
Manager cluster into two unconnected pieces. In the unlikely event that this occurs, both copies of Cisco Messaging Interface may become active, which leads to the possibility that they may simultaneously transmit SMDI messages to the voice-messaging system. If this happens, the collision could result in an erroneous message to the voice-messaging system, which may cause a call to be mishandled.
Cisco Unity Messaging integration

This chapter provides information about Cisco Unity messaging integration which comprises a communications solution that delivers voice messaging and unified messaging in a unified environment.

- Set up Cisco Unity and Cisco Unity connection, page 331
- System requirements, page 332
- Integration description, page 333
- Cisco Unified Communications Manager SIP trunk integration, page 334
- Secure the Voice Mail port, page 334

Set up Cisco Unity and Cisco Unity connection

Cisco Unity comprises a communications solution that delivers voice messaging and unified messaging in a unified environment.

Unified messaging means that users can manage all message types from the same inbox. Cisco Unity works in concert with an Exchange server or (for Cisco Unity 4.0 and later) a Domino server to collect and store all messages—both voice and e-mail—in one message facility. Users can then access voice and e-mail messages on a computer, through a touchtone phone, or over the Internet.

Steps to configure the Cisco Unity or Cisco Unity Connection voice-messaging systems are as follows.

**Procedure**

**Step 1** Ensure that you have met the system requirements for Cisco Unified Communications Manager, and Cisco Unity or Cisco Unity Connection.

System requirements, on page 332
Step 2 Add voice-mail ports (directory numbers) for each port that you are connecting to Cisco Unity or Cisco Unity Connection.

Step 3 Add a voice-mail pilot number for the voice-mail ports.

Step 4 Specify MWI and voice-mail extensions.

Step 5 Add the Voice Mail Port DNs to a line group.

Step 6 Add the line group that contains the Voice Mail Port DNs to a hunt list.

Step 7 Associate the hunt list that contains the line group with a hunt pilot.
   Note The hunt pilot must match the voice-mail pilot that is configured and used by the voice-mail profiles.

Step 8 Set up the voice-mail pilot number.

Step 9 Set up the voice-mail profile.

Step 10 Set up the voice-mail service parameters.

Step 11 Set up Cisco Unified Communications Manager authentication and encryption. For Cisco Unity, this applies to releases 4.0(5) and later.

Step 12 Test the integration.

Step 13 Integrate the secondary server for Cisco Unity failover (use when Cisco Unity failover is installed). This step does not apply to Cisco Unity Connection.

Step 14 Choose the auto-generated Cisco Unity or Cisco Unity Connection server in the Application Server Configuration window in Cisco Unified Communications Manager Administration.

Step 15 If you are using Cisco Unified Communications Manager Administration to configure voice-messaging users, create a Cisco Unity Connection voice mailbox.
   Tip You must configure both Cisco Unity Connection and Cisco Unified Communications Manager Administration to create voice mailboxes.
   Tip If you want to do so, you can use the import users functionality in Cisco Unity Connection to create users.

System requirements

The following lists provide requirements for your phone system and the Cisco Unity server. For specific version information, see the applicable Cisco Unified Communications Manager Integration Guide for Cisco Unity.

Phone System

- A Cisco Unified Communications applications server that consists of Cisco Unified Communications Manager software that is running on a Cisco Media Convergence Server (MCS) or customer-provided server that meets approved Cisco configuration standards
- Cisco licenses for all phone lines, IP phones, and other H.323-compliant devices or software (such as Cisco Virtual Phone and Microsoft NetMeeting clients) that will be connected to the network, as well as one license for each Cisco Unity port
- IP phones for the Cisco Unified Communications Manager extensions
- A LAN connection in each location where you will plug an IP phone into the network
• For multiple Cisco Unified Communications Manager clusters, capability for subscribers to dial an extension on another Cisco Unified Communications Manager cluster without having to dial a trunk access code or prefix.

Cisco Unity Server

• Cisco Unity system that was installed and made ready for the integration as described in the Cisco Unity Installation Guide.

• For SCCP integrations (not SIP trunk)—The applicable Cisco Unity-Unified CM TSP installed. For more information on compatible versions of the TSP, see the SCCP Compatibility Matrix: Cisco Unity, Cisco Unity-CM TSP, Cisco Unified CM, and Cisco Unified CM Express.

• A license that enables the appropriate number of voice-messaging ports.

Integration description

The integration uses the LAN to connect Cisco Unity and Cisco Unified Communications Manager. The gateway provides connections to the PSTN. The figure below shows the connections.

Figure 36: Connections Between the Phone System and Cisco Unity

Note

The following example applies only if the caller goes through the Cisco Unity Auto-Attendant. Most other calls get routed directly to the correct voice mailbox. For example, callers who call a subscriber and get forwarded to voice-messaging system go directly to the voice mailbox and can record a voice message. Subscribers who call in to check their voice messages from their own phones go directly to their voice mailbox and can listen to voice messages.

1 When an external call arrives, the Cisco gateway sends the call over the LAN to the machine on which Cisco Unified Communications Manager is installed.

2 For Cisco Unified Communications Manager lines that are configured to route calls to Cisco Unity, Cisco Unified Communications Manager routes the call to an available Cisco Unity extension.

3 Cisco Unity answers the call and plays the opening greeting.

4 During the opening greeting, the caller enters either the name of a subscriber or an extension; for example, 1234.

5 Cisco Unity notifies Cisco Unified Communications Manager that it has a call for extension 1234.

6 At this point, the path of the call depends on whether Cisco Unity is set up to perform supervised transfers or release transfers.
Cisco Unified Communications Manager SIP trunk integration

Cisco Unity Connection 1.1 and later support a SIP trunk integration with the Cisco Unified Communications Manager phone system when the Cisco Unified Communications Manager phone system has only phones that are running SIP. See the applicable Cisco Unified Communications Manager SIP Trunk Integration Guide for Cisco Unity Connection for more detailed information. Cisco Unity 4.2 and later also support SIP trunk integrations. See the applicable Cisco Unified Communications Manager SIP Trunk Integration Guide for Cisco Unity for more information. The following list describes a few tips that should be performed from the Cisco Unified Communications Manager Administration side when you are integrating the Cisco Unified Communications Manager phone system with Cisco Unity Connection or Cisco Unity by a SIP trunk:

• Create a SIP trunk that points to Cisco Unity and ensure that “Redirecting Number IE Delivery - Outbound” is checked. This instructs Cisco Unified Communications Manager to send the Diversion Header to Cisco Unity, so you access the correct voice mailbox.

• Cisco Unified Communications Manager SIP trunk integration applies to MWI. When you configure the SIP trunk security profile for the SIP voice-messaging trunk, check “Accept Unsolicited Notification.” This ensures that MWI will operate properly. You must enable “Accept Replaces Header” if you want to support transfers. This allows “REFER w/replaces” to be passed, which is used for Cisco Unity-initiated, supervised transfers.

• Assure that your phones support DTMF Relay per RFC-2833. Cisco Unity will support both OOB and RFC-2833.

• Define a route pattern (for example, 7555) and point that route pattern to the SIP trunk to Cisco Unity.

• Define a voice mail pilot (for example, 7555).

• Define a voice mail profile (for example, VM Profile 1) with the voice mail pilot that you defined in the previous step.

Note Make the voice mail profile that you defined in the preceding step the system default.

Secure the Voice Mail port

When you configure security for Cisco Unified Communications Manager voice mail ports and Cisco Unity SCCP devices, a TLS connection (handshake) opens for authenticated devices after each device accepts the certificate of the other device; likewise, the system sends SRTP streams between devices; that is, if you configure the devices for encryption.

When the device security mode equals authenticated or encrypted, the Cisco Unity-Unified CM TSP connects to Cisco Unified Communications Manager through the Cisco Unified Communications Manager TLS port. When the security mode equals non-secure, the Cisco Unity TSP connects to Cisco Unified Communications Manager through the Cisco Unified Communications Manager port. Cisco Unity Connection connects to Cisco Unified Communications Manager through the Cisco Unified Communications Manager TLS port.
Cisco DPA integration

This chapter provides information about the Cisco DPA 7630 and 7610 Voice Mail Gateways (DPA 7630/7610) which enable you to integrate Cisco Unified Communications Manager systems with Octel voice-messaging systems, which might also connect to either Definity or Meridian 1 PBX systems. This integration enables you to use your existing third-party telephony systems along with your Cisco IP telephony system.

For example, you can ensure that features such as message-waiting indicators (MWI) for Octel voice messages are properly set on Cisco Unified IP Phones (connected to Cisco Unified Communications Manager) and traditional telephony phones (connected to Definity or Meridian 1 PBX systems).

Using the DPA 7630/7610, you can integrate the following systems:

- Cisco Communications Manager 3.1(1) or higher
- Octel 200 and 300 voice-messaging systems (using APIC/NPIC integration)
- Octel 250 and 350 voice-messaging systems (using FLT-A/FLT-N integration)
- Definity G3 PBX systems (DPA 7630 only)
- Meridian 1 PBX systems (DPA 7610 only)

This section provides an overview of the DPA 7630/7610 and its interactions with the other components in traditional and IP telephony networks.

- DPA 7630/7610, page 335
- DPA 7630/7610 overview, page 336

DPA 7630/7610

The DPA 7630/7610 functions as a gateway between Cisco Unified Communications Manager and an Octel system (which may connect to a PBX system) and performs these tasks:

- Determines the call type from Cisco Unified Communications Manager and sends display, light, and ring messages to the Octel system.
- Determines when the Octel system is attempting to transfer, set message waiting indicators (MWI) and so on, and sends the appropriate messages to Cisco Unified Communications Manager.
• Converts dual-tone multi frequency (DTMF) tones to Skinny Client Control Protocol messages.
• Provides companding-law transcoding and voice compression.
• Performs Real-Time Transport Protocol (RTP) encapsulation of the voice message.

**DPA 7630/7610 overview**

With the Cisco DPA 7630/7610, you can integrate your existing Octel voice-messaging system with Cisco Unified Communications Manager and either a Definity PBX system or a Meridian 1 PBX system. If you have a Definity PBX, use the DPA 7630; if you have a Meridian 1 system, use the DPA 7610.

The DPA 7630/7610 functions by emulating digital phone or PBX systems. This capability allows it to appear like these devices to Cisco Unified Communications Manager, Octel, Definity, and Meridian 1 systems.

The following figure illustrates the Cisco DPA.

![Figure 37: Cisco DPA](image)

**When to use the DPA 7630/7610**

If you want to migrate your telephony system from a Definity G3 PBX or a Meridian 1 PBX to Cisco Unified Communications Manager, you must decide whether to do a complete cutover to Cisco Unified Communications Manager or to migrate slowly. If you do a complete cutover to Cisco Unified Communications Manager and Cisco voice-messaging solution, you do not need the DPA 7630/7610. However, if you are slowly migrating your systems, you might want to maintain some phones on the Definity or Meridian 1 PBX while you are installing new phones on the Cisco Unified Communications Manager system. You might want to use your existing Octel voice-messaging system with your Cisco Unified Communications Manager system. In these cases, the DPA 7630/7610 can assist your migration to Cisco Unified Communications Manager.

**When to use SMDI**

Because voice-messaging systems such as Octel were designed to integrate to only one PBX at a time, difficulty occurs with migration. To resolve this difficulty, many people use Simplified Message Desk Interface (SMDI), which was designed to enable integrated voice-messaging services to multiple clients.

To use SMDI, you must ensure that your voice-messaging system meets several qualifications:

• It must have sufficient database capacity to support two PBX systems simultaneously and to associate each mailbox with the correct PBX to send MWI information on the correct link.

• You must have the ability to physically connect the IP network to the voice-messaging system while maintaining the existing physical link to the PBX.
• It must support analog integration. SMDI primarily acts as an analog technology.

Additionally, SMDI requires reconfiguration of your existing telephony network.

**When not to use SMDI**

Be aware that SMDI might not be an option for you, particularly if you are using a digital interface on your Octel systems. Octel systems with digital line cards emulate digital phones and appear to the PBX as digital extensions, referred to as per-port or PBX integration cards (PIC). On PIC systems, the voice and data streams (for setting MWI) use the same path. The system sets and clears the MWIs via feature access codes on dedicated ports. Because these PIC ports use proprietary interfaces, you cannot use standard interfaces to connect them to the Cisco Unified Communications Manager system.

The DPA 7630/7610 can, however, translate these interfaces to enable communication among the Cisco Unified Communications Manager, Octel, and Definity or Meridian 1 systems. Depending on the needs of your network, you can choose among several different integration methods.
Part VII

System features

- Call Park and Directed Call Park, page 341
- Call Pickup, page 343
- Cisco Unified IP phone services, page 345
- Cisco Extension Mobility and phone login features, page 351
- Cisco Unified Communications Manager Assistant, page 353
This chapter provides information about the Call Park feature which allows you to place a call on hold, so it can be retrieved from another phone in the system. For example, if you are on an active call at your phone, you can park the call to a call park extension by pressing the Park softkey. Someone on another phone in your system can then dial the call park extension to retrieve the call.

Directed Call Park allows a user to transfer a call to an available user-selected directed call park number. A user can retrieve a parked call by dialing a configured retrieval prefix followed by the directed call park number where the call is parked.

Configure directed call park numbers in the Cisco Unified Communications Manager Directed Call Park Configuration window. You can configure phones that support the directed call park Busy Lamp Field (BLF) to monitor the busy/idle status of specific directed call park numbers. Users can also use the BLF to speed dial a directed call park number.
Call Pickup

This chapter provides information about the Call Pickup feature which allows users to answer calls that come in on a directory number other than their own.
CHAPTER 36

Cisco Unified IP phone services

This chapter provides information about IP phone services. Using Cisco Unified Communications Manager Administration, you can define and/or maintain IP phone services that can display on supported Cisco Unified IP Phones models. IP phone services comprise XML applications or Cisco-signed Java Midlets that enable the display of interactive content with text and graphics on some Cisco Unified IP Phones models.

Cisco Unified Communications Manager provides Cisco-provided default IP phone services, which install automatically with Cisco Unified Communications Manager. You can also create customized Cisco Unified IP Phone services for your site.

After you provision the IP phone services, you can perform the following tasks:

- Assign the service to phones, that is, if the service is not marked as an enterprise subscription
- Provision the IP phone service as a speed dial (service URL button) on the phone, that is, if the service is not marked as an enterprise subscription

Users can log in to the Cisco Unified CM User Options and subscribe to these services for their Cisco Unified IP Phones; that is, as long as these IP phone services are not classified as enterprise subscriptions.

- Configure Cisco Unified IP phone service, page 345
- Cisco Unified IP phone services overview, page 347
- Installation and upgrade considerations for IP phone services, page 348
- Phone support for IP phone services, page 348
- Guidelines and tips, page 349
- Dependency records, page 349

Configure Cisco Unified IP phone service

Using Cisco Unified Communications Manager Administration, you can define and/or maintain IP phone services that can display on supported Cisco Unified IP Phones models. IP phone services comprise XML applications or Cisco-signed Java Midlets that enable the display of interactive content with text and graphics on some Cisco Unified IP Phones models.
Cisco Unified Communications Manager provides Cisco-provided default IP phone services, which install automatically with Cisco Unified Communications Manager. You can also create customized Cisco Unified IP Phone applications for your site.

After you provision the IP phone services, you can perform the following tasks:

- Assign the service to phones, that is, if the service is not marked as an enterprise subscription
- Provision the IP phone service as a speed dial (service URL button) on the phone, that is, if the service is not marked as an enterprise subscription

Users can log on to the Cisco Unified CM User Options and subscribe to these services for their Cisco Unified IP Phones; that is, as long as these IP phone services are not classified as enterprise subscriptions.

To configure Cisco Unified IP Phone services refer to the following steps.

**Procedure**

**Step 1** Provision the Cisco Unified IP Phone Service, including the list of parameters that personalize the service. (Device > Device Settings > Phone Service) Cisco-provided default services display in the Find and List IP Phone Services Configuration window after a Cisco Unified Communications Manager installation or upgrade. If you want to do so, you can update these services. If you update these services, you may need to update the Service Provisioning drop-down list box.

Installation and upgrade considerations for IP phone services, on page 348

To determine the parameters for your IP phone service, see the documentation that supports your IP phone service.

**Step 2** Configure the Service Provisioning drop-down list box. How you configure this setting depends on the phone models that are in your network. If all phone models in your network can parse the service configuration information from the phone configuration file, you can choose Internal. If you have phone models in your network that cannot parse the service configuration information from the phone configuration file, choose Both. Choosing Both allows you to support phones that can parse the service information from the phone configuration file and phone models that can only obtain the service information from a service URL; some phone models, for example, the Cisco Unified IP Phone 7960, can only obtain the service information from a service URL; to support all phone models in your network, choose Both.

This drop-down list box displays in the Enterprise Parameter Configuration window (System > Enterprise Parameter), in the Common Phone Profile window (Device > Device Settings > Common Phone Profile), and in the Phone Configuration window (Device > Phone).

**Step 3** For phones that have Messages, Directory, or Service buttons/options, you can specify under which button/option on the phone the service will display. (You do this in the Phone Services Configuration window.) If you want the service to display as a speed dial button on the phone, create and customize a phone button template that includes the service URL button; then, assign the IP phone service to the service URL button. You can only add services as speed dials if the service is not marked as enterprise subscription.

**Step 4** Notify users that the Cisco Unified IP Phone Services are available. See the phone documentation for instructions on how users access Cisco Unified IP Phone services.
Cisco Unified IP phone services overview

Cisco Unified IP Phone services comprise XML applications or Cisco-signed Java Midlets that enable the display of interactive content with text and graphics on Cisco Unified IP Phones. Typical services that might be supplied to a phone include weather information, stock quotes, and news quotes.

With IP phone service provisioning, you can perform the following tasks:

- Configure how the phone provisions the service.
  You can specify whether the phone gets the service from its configuration file, whether the phone retrieves the service from a custom Service URL, or whether the phone supports both options.

- Configure whether the IP phone service displays on the phone.
  You can enable or disable a service in Cisco Unified Communications Manager Administration, which allows you to display or not display the service on the phone without deleting the service from the database.

  For example, if you do not want to display any call history information on the phone, choose Device > Device Settings > Phone Services, and uncheck the Enable check box for the Missed Calls, Received Calls, Placed Calls, and Intercom Calls in each configuration window.

- Configure where the IP phone services display on the phone.
  By default, for phones with Directory, Messages, or Services buttons/options, the service displays either under one of the buttons/options on the phone. If you want to do so, you can change this assignment in Cisco Unified Communications Manager Administration.

  If you want to display the IP phone service as a speed dial on the phone, you can do so. (See the Configure Cisco Unified IP phone service, on page 345.)

- Configure whether a service displays on all phones in the cluster that support services (or whether phone users can subscribe to the service via the Cisco Unified CM User Options).

  If the service is not marked as an enterprise subscription, you (or an end user) can subscribe the service to the phone; for example, you can subscribe a lobby phone or other shared devices to a service if the service is not marked as an enterprise subscription.

  If the service is marked as an enterprise subscription, the service displays on all phone in the cluster, unless you disable the service in Cisco Unified Communications Manager Administration (by unchecking the Enable check box in the Phone Services Configuration window).

  When the user clicks the Subscribe button, Cisco Unified Communications Manager builds a custom URL and stores it in the database for this subscription. The service then appears on the device services list.

- Configure a list of parameters for the IP phone service. These parameters personalize a service for an individual user. Examples of parameters include stock ticker symbols, city names, zip codes, or user IDs. To determine the parameters for your IP phone service, see the documentation that supports your IP phone service.

Tip
IP phone service provisioning allows you to install Cisco-signed Java MIDlets or XML applications on the phone. In addition, IP phone service provisioning provides Cisco-provided default services after an installation or upgrade.
Installation and upgrade considerations for IP phone services

If you provisioned services before a Cisco Unified Communications Manager upgrade, you may need to perform additional configuration tasks after the upgrade. For example, if you use a custom directory that points to a specific service URL, you may need to update the Service Provisioning drop-down list box.

If you upgrade Cisco Unified Communications Manager and your services do not display or work on the phone, change the Service Provisioning setting to Both.

Cisco Unified Communications Manager automatically provisions Cisco-provided default services. These services display in the Find and List IP Phone Services window (Device > Device Settings > Phone Services). To update these services, click the link in the window. You can change the name of the service, where the default service displays on the phone, and the service URL. If you change the service URL for the default services, choose Both from the Service Provisioning drop-down list box, which allows you to support various phone models in your network; that is, your network can support phone models that can retrieve the service information from the phone configuration file and phone models that can retrieve the service information from an external service URL (for example, the Cisco Unified IP Phone 7960).

Phone support for IP phone services

Consider the following process, which indicates how a Cisco Unified IP Phone supports XML services and Cisco-signed Java MIDlets:

1. The phone receives its configuration file after a reset, restart, or boot up and updates its local service configuration if changes exist.

2. If any service in the configuration file is a Cisco-signed Java MIDlet, the phone compares the provisioned Java MIDlet services to the list of installed Java MIDlet services to determine whether the services need to be installed, uninstalled, upgraded or downgraded. The phone automatically attempts to perform the necessary actions. If the phone fails to install the Java MIDlet on the phone, the phone retries to perform the necessary actions.

3. For XML services, the information in the phone configuration file points to a web script/file, which returns an XML object. Because these services are not installed on the phone, the phone invokes the service URL only when the user selects the option for the service on the phone.

The phone automatically uninstalls the Cisco-signed Java MIDlet under the following circumstances:

- When Cisco Extension Mobility is used to change the current active user on the phones, which occurs during login and logout
- If a phone user is not logged into the phone via Cisco Extension Mobility, but the Owner User ID field is updated in Cisco Unified Communications Manager Administration (which changes the current active user for the device)
- If the phone registers with a different Cisco Unified Communications Manager cluster that does not support Cisco-signed Java MIDlets (or if the other cluster has a different service configuration for the device)
- If the configuration is cleared on the phone by any method; for example, via the Settings menu on the phone or a factory reset on the phone.
Cisco Unified IP Phone models support IP phone services provisioning differently; for example, the Cisco Unified IP Phone 7941G, 7941G-GE, 7961G, 7961G-GE, 7942G, 7962G, 7945G, 7965G, 7970G, 7971G, and 7975G can parse the service information from the phone configuration file, can support movement of services to the Message, Directory, and Services buttons/options on the phone, and so on; for example, the Cisco Unified IP Phones 7906G, 7911G, and 7931G do not support Cisco-signed Java MIDlets, but these phones can parse the service information from the phone configuration file. To determine the service provisioning support for your phone model, see the Cisco Unified IP Phone Administration Guide that supports your phone model and this release of Cisco Unified Communications Manager.

Guidelines and tips

Consider the following guidelines and tips when you provision IP phone services in Cisco Unified Communications Manager Administration:

To minimize the impact to Cisco Unified Communications Manager performance and call processing, do not put IP phone services on any Cisco Unified Communications Manager server at your site or any server that is associated with Cisco Unified Communications Manager, such as the TFTP server or publisher database server.

If you do not want to display the service on the phone, uncheck the Enable check box in the IP Phone Services Configuration window (Device > Device Settings > Phone Services).

If you want to display IP phone services on a different button than the button that is specified as the default, update the Services Type setting.

If you change the default service URL for a Cisco-provided default service, for example, you change the service URL for the corporate directory from Application: Cisco/CorporateDirectory to a custom URL, make sure that you choose Both from the Service Provisioning drop-down list box. (See Configure Cisco Unified IP phone service, on page 345.)

If you want to do so, you can configure the Services Provisioning enterprise parameter, which applies the configuration to all phones in the cluster that support IP phone services. (In Cisco Unified Communications Manager Administration, choose System > Enterprise Parameter.)

If an end user or you subscribe to a disabled service, the phone does not display the service on the button/menu.

If you upgrade Cisco Unified Communications Manager and your services do not display or work on the phone, change the Service Provisioning setting to Both.

Cisco Unified Communications Manager allows you to create two or more IP phone services with identical names. Cisco recommends that you do not do so unless most or all phone users are advanced, or unless an administrator always configures the IP phones. Be aware that if AXL or any third-party tool accesses the list of IP phone services for configuration, you must use unique names for IP phone services.

Dependency records

To find devices that a specific Cisco Unified IP Phone service is using, in the IP Phone Services Configuration window in Cisco Unified Communications Manager Administration, choose Dependency Records from the
Related Links drop-down list box and click Go. The Dependency Records Summary window displays information about devices that are using the Cisco Unified IP Phone Service. To find out more information about the device, click the device, and the Dependency Records Details window displays. If the dependency records are not enabled for the system, the Dependency Records Summary window displays a message.
Cisco Extension Mobility and phone login features

This chapter provides information about the Cisco Extension Mobility feature which allows users to configure any Cisco Unified IP Phone 7940 or Cisco Unified IP Phone 7960 as their own, on a temporary basis, by logging in to that phone. After a user logs in, the phone adopts the individual user default device profile information, including line numbers, speed dials, services links, and other user-specific properties of a phone. For example, when user A occupies a desk and logs in to the phone, that user directory number(s), services, speed dials, and other properties appear on that phone; but when user B uses the same desk at a different time, user B information displays. The Cisco Extension Mobility feature dynamically configures a phone according to the current user.

Previously, only administrators could change phone settings through Cisco Unified Communications Manager Administration. The Cisco Extension Mobility feature allows users to change phone settings themselves without accessing Cisco Unified Communications Manager Administration. Instead, when users authenticate themselves at the phone, a login service performs the administrative updates.

The programmable login service enforces a variety of uses, including duration limits on phone configuration (persistence) and authorization to log in to a particular phone. A Cisco IP Phone XML service provides the user interface to the login service that is provided in this release.
This chapter provides information about the Cisco Unified Communications Manager Assistant feature which enables managers and their assistants to work together more effectively. Cisco Unified Communications Manager Assistant supports two modes of operation: proxy line support and shared line support. Both modes support multiple calls per line for the manager. The Cisco IP Manager Assistant service supports both proxy line and shared line support.

Both modes of Cisco Unified Communications Manager Assistant comprise enhancements to phone capabilities for the manager and desktop interfaces that are primarily for the use of the assistant. Cisco Unified Communications Manager Assistant with proxy line support includes a call-routing service.

With Cisco Unified Communications Manager Assistant with proxy line support, the service intercepts calls that are made to managers and routes them to selected assistants, to managers, or to other targets based on preconfigured call filters. The manager can change the call routing dynamically; for example, with a softkey press on the phone, the manager can instruct the service to route all calls to the assistant and can receive status on these calls.

Cisco Unified Communications Manager users comprise managers and assistants. The Cisco Unified Communications Manager Assistant with proxy line support routing service intercepts a manager user calls and routes them appropriately (Cisco Unified Communications Manager Assistant with shared line support does not support routing). An assistant user handles calls on behalf of a manager. Cisco Unified Communications Manager Assistant comprises features for managers and features for assistants.
PART VIII

Devices and protocols

- Cisco Unified Communications Manager voice gateways overview, page 357
- IP telephony protocols, page 381
- Session Initiation Protocol, page 397
- Cisco Unified Communications Manager trunk types, page 449
- Cisco Unified IP phones, page 459
- Video telephony, page 543
- Computer Telephony Integration, page 577
- Cisco ATA 186, page 587
- Administrative tools overview, page 589
This chapter provides information about Cisco Unified Communications gateways which enable Cisco Unified Communications Manager to communicate with non-IP telecommunications devices. Cisco Unified Communications Manager supports several types of voice gateways.

- Set up gateway, page 357
- Set up MGCP BRI gateway, page 358
- Cisco voice gateways, page 359
- Gateways dial plans and route groups, page 374
- Gateways and the Local Route Groups feature, page 375
- Gateways and the Calling Party Normalization feature, page 375
- Apply the international escape character to inbound calls over H.323 trunks, page 376
- Gateway failover and fallback, page 376
- Transfer calls between gateways, page 378
- H.235 support for gateways, page 380

**Set up gateway**

Gateways enable Cisco Unified Communications Manager to communicate with non-IP telecommunications devices. The following steps are required to configure gateways in Cisco Unified Communications Manager.
Set up MGCP BRI gateway

The following steps are required to configure a BRI gateway in Cisco Unified Communications Manager.

**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Install and configure the gateway and voice modules in the network.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Gather the information that you need to configure the gateway to operate with Cisco Unified Communications Manager and to configure the trunk interface to the PSTN or external non-IP telephony device.</td>
</tr>
<tr>
<td>Step 3</td>
<td>On the gateway, perform any required configuration steps.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Add and configure the gateway in Cisco Unified Communications Manager Administration.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Add and configure ports on the gateway.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Configure the dial plan for the gateway for routing calls out to the PSTN or other destinations. This configuration can include setting up a route group, route list, and route pattern for the gateway in Cisco Unified Communications Manager or, for some gateways, configuring the dial plan on the gateway itself.</td>
</tr>
<tr>
<td>Step 7</td>
<td>Reset the gateway to apply the configuration settings.</td>
</tr>
</tbody>
</table>

**Tip** To get to the default web pages for gateway devices, you can use the IP address of that gateway. Make your hyperlink url = http://x.x.x.x/, where x.x.x.x specifies the dot-form IP address of the device. The web page for each gateway contains device information and the real-time status of the gateway.
Cisco voice gateways

Cisco Unified Communications Manager supports several types of Cisco Unified Communications gateways. Gateways use call control protocols to communicate with the PSTN and other non-IP telecommunications devices, such as private branch exchanges (PBXs), key systems, analog phones, fax machines, and modems.

Trunk interfaces specify how the gateway communicates with the PSTN or other external devices by using time-division-multiplexing (TDM) signaling. Cisco Unified Communications Manager and Cisco gateways use a variety of TDM interfaces, but supported TDM interfaces vary by gateway model.

The following list provides available interfaces that Cisco Unified Communications Manager supports with MGCP gateways:

- Foreign Exchange Office (FXO)
- Foreign Exchange Station (FXS)
- T1 Channel Associated Signaling (CAS) receive and transmit or ear and mouth (E&M)
- Basic Rate Interface (BRI) Q.931
- T1 PRI-North American ISDN Primary Rate Interface (PRI)
- E1 PRI-European ISDN Primary Rate Interface (PRI)

The following list provides available interfaces that Cisco Unified Communications Manager supports with H.323 gateways:

- FXO
- FXS
- E&M
- Analog Direct Inward Dialing (DID)
- Centralized Automatic Message Accounting (CAMA)
- BRI Q.931
- BRI QSIG-Q signaling protocol that is based on ISDN standards
- T1 CAS FXS, FXO, and E&M
- T1 FGD
- T1/E1 PRI
- T1 PRI NFAS
- T1/E1 QSIG
- E1 R2
- J1

The following list provides available interfaces that Cisco Unified Communications Manager supports with SCCP gateways:

- FXS
Cisco Unified Communications Manager can use H.323 gateways that support E1 CAS, but you must configure the E1 CAS interface on the gateway.

**Standalone voice gateways**

This section describes these standalone, application-specific gateway models that are supported for use with Cisco Unified Communications Manager.

**Cisco VG248 Analog Phone Gateway**

The Cisco VG248 Analog Phone Gateway has a standalone, 19-inch rack-mounted chassis with 48-FXS ports. This product allows on-premise analog telephones, fax machines, modems, voice-messaging systems, and speakerphones to register with a single Cisco Unified Communications Manager system.

**Cisco VG248 Analog Phone Connectivity**

The Cisco VG248 Analog Phone Gateway communicates with Cisco Unified Communications Manager by using the Skinny Client Control Protocol to allow support for the following supplementary services features for analog phones:

- Call transfer
- Conference
- Call waiting (with calling party ID display)
- Hold (including switch between parties on hold)
- Music on hold
- Call forward all
- Send all calls to voice-messaging system
- Group call pickup
- Voice-messaging system message waiting indication
- Speed dial (maximum of 9 speed dials)
- Last number redial
- Cisco fax relay
- Dynamic port and device status that is available from Cisco Unified Communications Manager

**Cisco VGC Phone Device Types**

All Cisco VG248 ports and units appear as distinct devices in Cisco Unified Communications Manager with the device type “Cisco VGC Phone.” Cisco Unified Communications Manager recognizes and configures each port as a phone.

**Fax and Modem Connectivity**

The Cisco VG248 supports legacy fax machines and modems. When using fax machines, the Cisco VG248 uses either the Cisco fax relay or pass-through/up speed technology to transfer faxes across the network with high reliability.
You can connect any modem to the Cisco VG248 by using pass-through mode.

**Voice-Mail Connectivity**

The Cisco VG248 generates call information by using the Simplified Message Desk Interface (SMDI) format for all calls that are ringing on any of the 48 analog lines that connect to it. It will also pass on SMDI call information from other Cisco VG248s, or from a legacy PBX, to the voice-messaging system. Any commands for message-waiting indicators get sent to Cisco Unified Communications Manager and to any other attached SMDI hosts.

This mechanism allows for many new configurations when SMDI-based voice-messaging systems are used, including:

- You can share a single voice-messaging system between Cisco Unified Communications Manager and a legacy PBX.
- Voice-messaging system and Cisco VG248 can function remotely in a centralized call-processing model.
- Multiple clusters can use a single voice-messaging system, by using one Cisco VG248 per cluster.
- Configure multiple voice-messaging systems in a single cluster because the Cisco VG248 generates SMDI call information rather than the Cisco Unified Communications Manager.

**Cisco VG248 Time Device**

The Cisco VG248 contains a real-time clock that is persistent across power cycles and restarts. The real-time clock gets set for the first time when the device registers with Cisco Unified Communications Manager. The clock gets set by using the DefineDateTime Skinny message that Cisco Unified Communications Manager sends. After a power cycle or restart, the clock resets when the Cisco VG248 receives the DefineDateTime message from Cisco Unified Communications Manager and then resets no more than once per hour thereafter.

**Cisco VG248 Configuration File Updates**

The Cisco VG248 queries the TFTP server to access the configuration files for the device. The configuration files update whenever you modify the configuration of the Cisco VG248 via Cisco Unified Communications Manager.

**Cisco VG224 Analog Phone Gateway**

The Cisco VG224 Analog Phone Gateway, which has a standalone, 17-inch rack-mounted chassis with 24-FXS ports, allows on-premise analog telephones, fax machines, modems, and speakerphones to register with Cisco Unified Communications Manager.

This gateway supports the H.323, MGCP, SCCP, SIP, and T.38 fax relay.

**Cisco Voice Gateway 200**

The Cisco Unified Communications Voice Gateway (VG200) provides a 10/100BaseT Ethernet port for connection to the data network. The following list gives available telephony connections:

- 1 to 4 FXO ports for connecting to a central office or PBX
- 1 to 4 FXS ports for connecting to POTS telephony devices
- 1 or 2 Digital Access T1 ports for connecting to the PSTN
• 1 or 2 Digital Access PRI ports for connecting to the PSTN
• MGCP or H.323 interface to Cisco Unified Communications Manager
  ◦ MGCP mode supports T1/E1 PRI, T1 CAS, FXS, FXO. (Only the user side supports BRI.)
  ◦ H.323 mode supports E1/T1 PRI, E1/T1 CAS, FXS, and FXO. H.323 mode supports E&M, fax relay, and G.711 modem.

The MGCP VG200 integration with legacy voice-messaging systems allows the Cisco Unified Communications Manager to associate a port with a voice mailbox and connection.

**MGCP BRI call connections**

Previously, gateways used H.323 signaling to Cisco Unified Communications Manager to provide interfaces to the public switched telephone network (PSTN) for BRI ISDN connections.

Now, Cisco Unified Communications Manager can use a Media Gateway Control Protocol (MGCP) gateway to handle BRI ISDN connections to the PSTN and to provide a centrally administered gateway interface. Cisco Unified Communications Manager uses logical connections to exchange MGCP and ISDN Q.931 messages with the gateway. This connection uses a User Datagram Protocol (UDP) logical connection for exchanging MGCP messages and a Transmission Control Protocol (TCP) connection for the backhaul ISDN Q.931 messages.

The following figure shows a typical scenario that centralizes call processing for remote-site BRI trunk gateways that connect to the PSTN. When a call arrives from or goes to the PSTN over the BRI trunk, the Cisco Unified Communications Manager and the gateway (based on an IOS router) exchange ISDN Q.931 messages across the WAN.

*Figure 38: Topology Shows a Scenario by Using MGCP BRI Interfaces*

---

**Note**

The BRI gateway supports MGCP BRI backhaul for BRI trunk only. It does not support BRI phone or station. The IOS gateway supports BRI phones that use Skinny Client Control Protocol.
Switch-based gateways

Several telephony modules for the Cisco Catalyst 4000 and 6000 family switches act as telephony gateways. You can use existing Cisco Catalyst 4000 or 6000 family devices to implement IP telephony in your network by using the following voice gateway modules:

- Install Catalyst 6000 voice gateway modules that are line cards in any Cisco Catalyst 6000 or 6500 series switch.
- Install the Catalyst 4000 access gateway module in any Catalyst 4000 or 4500 series switch.

Cisco Catalyst 6000 8-Port Voice T1/E1 and Services Module

The Cisco Catalyst 6000 8-Port Voice T1/E1 and Services Modules provide the following features:

- 8 ports for providing
  - Digital T1/E1 connectivity to the PSTN (T1/E1 PRI or T1 CAS)
  - Digital signal processor (DSP) resources for transcoding and conferencing
- MGCP interface to Cisco Unified Communications Manager
- Connection to a voice-messaging system (using T1 CAS)

Users have the flexibility to use ports on a T1 module for T1 connections or as network resources for voice services. Similarly, the E1 module provides ports for E1 connections or as network resources. The ports can serve as T1/E1 interfaces, or the ports will support transcoding or conferencing.

Note

Either module supports DSP features on any port, but T1 modules cannot be configured for E1 ports, and E1 modules cannot be configured for T1 ports.

Similar to the Cisco MGCP-controlled gateways with FXS ports, the Cisco 6608 T1 CAS gateway supports hookflash transfer. Hookflash transfer defines a signaling procedure that allows a device, such as a voice-messaging system, to transfer to another destination. While the device is connected to Cisco Unified Communications Manager through a T1 CAS gateway, the device performs a hookflash procedure to transfer the call to another destination. Cisco Unified Communications Manager responds to the hookflash by using a blind transfer to move the call. When the call transfer completes, the voice channel that connected the original call to the device gets released.

Note

Only E&M T1 ports support hookflash transfer.

Cisco Catalyst 6000 24 Port FXS Analog Interface Module

The Cisco Catalyst 6000 24 Port FXS Analog Interface Module provides the following features:

- 24 Port RJ-21 FXS module
- V.34/V.90 modem, voice-messaging system, IVR, POTS
Cisco Communication Media Module

The Cisco Communication Media Module (CMM), which is a Catalyst 6500 line card, provides T1 and E1 gateways that allow organizations to connect their existing TDM network to their IP communications network. The Cisco CMM provides connectivity to the PSTN also. You can configure the Cisco CMM, which provides an MGCP, H.323, or SIP interface to Cisco Unified Communications Manager, with the following interface and service modules:

- 6-port T1 interface module for connecting to the PSTN or a PBX
- 6-port E1 interface module for connecting to the PSTN or a PBX
- 24-port FXS interface module for connecting to POTS telephony devices

**Note**

The Cisco CMM fits in the Cisco 7600 platform chassis.

Cisco Catalyst 4000 Access Gateway Module

The Cisco Catalyst 4000 Access Gateway Module provides an MGCP or H.323 gateway interface to Cisco Unified Communications Manager. You can configure this module with the following interface and service modules:

- 6 ports for FXS and FXO
- 2 T1/E1 ports for Digital Access PRI and Digital Access T1

Cisco Catalyst 4224 Voice Gateway Switch

The Cisco Catalyst 4224 Voice Gateway Switch provides a single-box solution for small branch offices. The Catalyst 4224 provides switching, IP routing, and PSTN voice-gateway services by using onboard digital signal processors (DSPs). The Catalyst 4224 has four slots that you can configure with multiflex voice and WAN interface cards to provide up to 24 ports. These ports can support the following voice capabilities:

- FXS ports for POTS telephony devices
- FXO ports for PSTN connections
- T1 or E1 ports for Digital Access PRI, and Digital Access T1 services
The Cisco Catalyst 4224 Access Gateway Switch provides an MGCP or H.323 interface to Cisco Unified Communications Manager.

H.323 Gateways

H.323 devices comply with the H.323 communications standards and enable video conferencing over LANs and other packet-switched networks. You can add third-party H.323 devices or other Cisco devices that support H.323 (such as the Cisco 2600 series, 3600 series, or 5300 series gateways).

Cisco IOS H.323 Gateways

Cisco IOS H.323 gateways such as the Cisco 2600, 3600, 1751, 1760, 3810 V3, 7200 7500, AS5300, and VG200 provide full-featured routing capabilities. See the documentation for each of these gateway types for information about supported voice gateway features and configuration.

Outbound FastStart call connections

Calls that are placed from IP phones over large WAN topologies can experience voice clipping when the called party goes off hook to answer the call. When H.323 trunks or gateways are separated from the Cisco Unified Communications Manager server, significant delays can occur because of the many H.245 messages that are exchanged when a call is set up.

With the FastStart feature, information that is required to complete a media connection between two parties gets exchanged during the H.225 portion of call setup, and this exchange eliminates the need for H.245 messages. The connection experiences one roundtrip WAN delay during call setup, and the calling party does not receive voice clipping when the called party answers the call.

Cisco Unified Communications Manager uses media termination points (MTP) for making an H.323 outbound FastStart call. Cisco Unified Communications Manager starts an outbound FastStart call by allocating an MTP and opening the receive channel. Next, the H.323 Fast Connect procedure sends the SETUP message with a FastStart element to the called endpoint. The FastStart element includes information about the receiving channel for the MTP.

The called endpoint accepts the H.323 Fast Connect procedure by sending a CALL PROCEEDING, PROGRESS, ALERT, or CONNECT message that contains a FastStart element. When Cisco Unified Communications Manager receives the FastStart element, it connects the media immediately and avoids the delays with the usual exchange of H.245 messages.

The called endpoint can refuse the H.323 Fast Connect procedure by not returning the FastStart element in any of the messages up to and including the CONNECT message. In this case, the Cisco Unified Communications Manager handles the call as a normal call and uses the MTP for subsequent media cut-through.

The Outbound FastStart feature requires an MTP. If an MTP is not available when the call is set up, the call continues without FastStart and with no supplementary services. If you want all calls to use FastStart only, you can set the service parameter called “Fail call if MTP allocation fails,” which is located in the Cluster Wide Parameters (Device-H323) portion of the service parameters for the Cisco Unified CallManager service. When you set this parameter to True, the system rejects calls when no MTP is available.

Voice gateway model summary

The following table summarizes Cisco voice gateways that Cisco Unified Communications Manager supports with information about the supported signaling protocols, trunk interfaces, and port types.
### Table 29: Overview of Supported Voice Gateways, Protocols, Trunk Interfaces, and Port Types

<table>
<thead>
<tr>
<th>Gateway Model</th>
<th>Supported Signaling Protocols</th>
<th>Trunk Interfaces</th>
<th>Port Types</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS Integrated Routers</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cisco 1751 and Cisco 1760</td>
<td>H.323 and SIP</td>
<td>FXS</td>
<td>Loopstart or groundstart</td>
<td>Basic calls only</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FXO</td>
<td>Loopstart or groundstart</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>E&amp;M</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Analog DID</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>CAMA</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>BRI</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>BRI QSIG</td>
<td></td>
<td>Basic calls only</td>
</tr>
<tr>
<td></td>
<td></td>
<td>T1 CAS (E&amp;M, FXS, FXO)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>E1 R2</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>T1/E1 QSIG</td>
<td></td>
<td>Basic calls only</td>
</tr>
<tr>
<td></td>
<td></td>
<td>T1/E1 PRI</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>MGCP</td>
<td>FXS</td>
<td>Loopstart only</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Basic calls only</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>FXO</td>
<td>Loopstart or groundstart</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>No caller ID</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>BRI</td>
<td>User side only; no QSIG</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>support</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>T1 CAS (E&amp;M)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>T1/E1 QSIG</td>
<td>Supplementary Services</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cisco 2600, 2600XM series, 2691, 3700 series</td>
<td>H.323 and SIP</td>
<td>FXS</td>
<td>Loopstart or groundstart</td>
<td></td>
</tr>
<tr>
<td>Gateway Model</td>
<td>Supported Signaling Protocols</td>
<td>Trunk Interfaces</td>
<td>Port Types</td>
<td>Notes</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------------------------</td>
<td>-----------------</td>
<td>------------</td>
<td>-------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FXO</td>
<td>Loopstart or groundstart</td>
<td>Basic calls only</td>
</tr>
<tr>
<td></td>
<td></td>
<td>E&amp;M</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Analog DID</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>CAMA</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>BRI</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>BRI QSIG</td>
<td></td>
<td>Basic calls only</td>
</tr>
<tr>
<td></td>
<td></td>
<td>T1 CAS (E&amp;M, FXS, FXO)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>T1 FGD</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>E1 CAS</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>E1 R2</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>T1/E1 QSIG</td>
<td></td>
<td>Basic calls only</td>
</tr>
<tr>
<td></td>
<td></td>
<td>T1/E1 PRI</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>T1 PRI NFAS</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>T1 PRI (Megacom/SDN)</td>
<td></td>
<td>Per T1 port only; not per call</td>
</tr>
<tr>
<td></td>
<td>MGCP</td>
<td>FXS</td>
<td>Loopstart only</td>
<td>Basic calls only</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FXO</td>
<td>Loopstart or groundstart</td>
<td>No caller ID</td>
</tr>
<tr>
<td></td>
<td></td>
<td>BRI</td>
<td></td>
<td>Only 2600XM/2691 support MGCP BRI; User side only; no QSIG support</td>
</tr>
<tr>
<td></td>
<td></td>
<td>T1 CAS (E&amp;M)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>T1/E1 QSIG</td>
<td></td>
<td>Supplementary Services</td>
</tr>
<tr>
<td></td>
<td></td>
<td>T1/E1 PRI</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gateway Model</td>
<td>Supported Signaling Protocols</td>
<td>Trunk Interfaces</td>
<td>Port Types</td>
<td>Notes</td>
</tr>
<tr>
<td>------------------------</td>
<td>-------------------------------</td>
<td>------------------</td>
<td>----------------------------------</td>
<td>------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>T1 PRI (Megacom/SDN)</td>
<td>Per call</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SCCP</td>
<td>BRI</td>
<td>DoD STE BRI phones only; single-B-channel</td>
<td></td>
</tr>
<tr>
<td>Cisco 3600 series</td>
<td>H.323 and SIP</td>
<td>FXS</td>
<td>Loopstart or groundstart</td>
<td>Basic calls only</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FXO</td>
<td>Loopstart or groundstart</td>
<td></td>
</tr>
<tr>
<td></td>
<td>E&amp;M</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Analog DID</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CAMA</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>BRI</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>BRI QSIG</td>
<td>Basic calls only</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>T1 CAS (E&amp;M, FXS, FXO)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>T1 FGD</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>E1 CAS</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>E1 R2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>T1/E1 QSIG</td>
<td>Basic calls only</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>T1/E1 PRI</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>T1 PRI NFAS</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>T1 PRI (Megacom/SDN)</td>
<td>Per T1 port only; not per call</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>MGCP</td>
<td>FXS</td>
<td>Loopstart only</td>
<td>Basic calls only</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Loopstart or groundstart</td>
<td>No caller ID</td>
</tr>
<tr>
<td>Gateway Model</td>
<td>Supported Signaling Protocols</td>
<td>Trunk Interfaces</td>
<td>Port Types</td>
<td>Notes</td>
</tr>
<tr>
<td>------------------------------------------</td>
<td>-------------------------------</td>
<td>------------------</td>
<td>------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>BRI</td>
<td></td>
<td></td>
<td></td>
<td>Only 3640/3660 and some interface cards support MGCP BRI; User side only; no QSIG support</td>
</tr>
<tr>
<td>T1 CAS (E&amp;M)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>T1/E1 QSIG</td>
<td></td>
<td></td>
<td></td>
<td>Supplementary Services</td>
</tr>
<tr>
<td>T1/E1 PRI</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>T1 PRI (Megacom/SDN)</td>
<td></td>
<td></td>
<td></td>
<td>Per call</td>
</tr>
<tr>
<td>Cisco 2800 and 3800 series</td>
<td>H.323 and SIP</td>
<td>FXS</td>
<td>Loopstart or groundstart</td>
<td>Basic calls only</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FXO</td>
<td>Loopstart or groundstart</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>E&amp;M</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Analog DID</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>CAMA</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>BRI</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>BRI QSIG</td>
<td></td>
<td>Basic calls only</td>
</tr>
<tr>
<td></td>
<td></td>
<td>T1 CAS (E&amp;M, FXS, FXO)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>T1 FGD</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>E1 CAS</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>E1 R2</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>T1/E1 QSIG</td>
<td></td>
<td>Basic calls only</td>
</tr>
<tr>
<td></td>
<td></td>
<td>T1/E1 PRI</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>T1 PRI NFAS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gateway Model</td>
<td>Supported Signaling Protocols</td>
<td>Trunk Interfaces</td>
<td>Port Types</td>
<td>Notes</td>
</tr>
<tr>
<td>--------------------</td>
<td>--------------------------------</td>
<td>------------------</td>
<td>------------</td>
<td>---------------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>T1 PRI (Megacom/SDN)</td>
<td>Per T1 port only; not per call</td>
<td></td>
</tr>
<tr>
<td></td>
<td>MGCP</td>
<td>FXS</td>
<td>Loopstart only</td>
<td>Basic calls only</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FXO</td>
<td>Loopstart or groundstart</td>
<td>No caller ID</td>
</tr>
<tr>
<td></td>
<td></td>
<td>BRI</td>
<td>User side only; no QSIG support</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>T1 CAS (EM)</td>
<td>Supplementary Services</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>T1/E1 QSIG</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>T1/E1 PRI</td>
<td>Per call</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SCCP</td>
<td>FXS</td>
<td>T1 FGD</td>
<td>T1 FGD</td>
</tr>
<tr>
<td>Cisco 7200 series</td>
<td>H.323</td>
<td>T1 CAS (E&amp;M, FXS, FXO)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>T1 FGD</td>
<td>E1 R2</td>
<td>T1/E1 QSIG</td>
</tr>
<tr>
<td></td>
<td></td>
<td>T1 FGD</td>
<td>E1 R2</td>
<td>T1/E1 PRI</td>
</tr>
<tr>
<td>Cisco 5000 series</td>
<td>H.323 and SIP</td>
<td>T1 CAS (E&amp;M, FXS, FXO)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>T1 FGD</td>
<td>T1 FGD</td>
<td>T1/E1 QSIG</td>
</tr>
<tr>
<td></td>
<td></td>
<td>T1 FGD</td>
<td>E1 R2</td>
<td>T1/E1 PRI</td>
</tr>
</tbody>
</table>

Cisco Standalone Voice Gateways
<table>
<thead>
<tr>
<th>Gateway Model</th>
<th>Supported Signaling Protocols</th>
<th>Trunk Interfaces</th>
<th>Port Types</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco VG224 Analog Gateway</td>
<td>H.323, MGCP, and SIP</td>
<td>FXS</td>
<td></td>
<td>Basic calls only</td>
</tr>
<tr>
<td></td>
<td>SCCP</td>
<td>FXS</td>
<td></td>
<td>Supplementary Services</td>
</tr>
<tr>
<td>Cisco VG248 Analog Gateway</td>
<td>SCCP</td>
<td>FXS</td>
<td></td>
<td>Supplementary Services</td>
</tr>
<tr>
<td>Cisco VG200 Gateway</td>
<td>H.323 and SIP</td>
<td>FXS</td>
<td>Loopstart or groundstart</td>
<td>Basic calls only</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FXO</td>
<td>Loopstart or groundstart</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>E&amp;M</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Analog DID</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CAMA</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>BRI</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>BRI QSIG</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>T1 CAS (E&amp;M, FXS, FXO)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>T1 FGD</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>E1 CAS</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>E1 R2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>T1/E1 QSIG</td>
<td></td>
<td></td>
<td>Basic calls only</td>
</tr>
<tr>
<td></td>
<td>T1/E1 PRI</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>T1 PRI NFAS</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>T1 PRI (Megacom/SDN)</td>
<td></td>
<td></td>
<td>Per T1 port only; not per call</td>
</tr>
<tr>
<td></td>
<td>MGCP</td>
<td>FXS</td>
<td>Loopstart only</td>
<td>Basic calls only</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FXO</td>
<td>Loopstart or groundstart</td>
<td>No caller ID</td>
</tr>
<tr>
<td>Gateway Model</td>
<td>Supported Signaling Protocols</td>
<td>Trunk Interfaces</td>
<td>Port Types</td>
<td>Notes</td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td>------------------------------</td>
<td>------------------</td>
<td>---------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>Only 2600XM/2691 support MGCP BRI; Userside only; no QSIG support</td>
<td>BRI</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>T1 CAS (E&amp;M)</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>T1/E1 QSIG</strong></td>
<td></td>
<td></td>
<td></td>
<td>Supplementary Services</td>
</tr>
<tr>
<td><strong>T1/E1 PRI</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>T1 PRI (Megacom/SDN)</strong></td>
<td></td>
<td></td>
<td></td>
<td>Per call</td>
</tr>
<tr>
<td>Cisco Access Analog Trunk Gateway (AT-2, AT-4, AT-8)</td>
<td>SCCP</td>
<td>FXO</td>
<td>Loop start</td>
<td></td>
</tr>
<tr>
<td>Cisco Access Analog Station Gateway (AS-2, AS-4, AS-8)</td>
<td>SCCP</td>
<td>FXS</td>
<td></td>
<td>Supplementary Services</td>
</tr>
<tr>
<td>Cisco Catalyst Voice Gateway Modules</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cisco Communication Media Module (WS-X6600-24FXS)</td>
<td>MGCP or H.323</td>
<td>FXS</td>
<td></td>
<td>Basic calls only</td>
</tr>
<tr>
<td>Cisco Communication Media Module (WS-X6600-6T1)</td>
<td>H.323</td>
<td>T1 CAS (E&amp;M)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>T1 PRI</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>T1 QSIG</td>
<td>Basic calls only</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>T1 PRI NFAS</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>MGCP</td>
<td>T1 CAS (E&amp;M)</td>
<td>Supplementary Services</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>T1 QSIG</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>T1 PRI</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cisco Communication Media Module (WS-X6600-6E1)</td>
<td>H.323</td>
<td>E1 PRI</td>
<td></td>
<td>Basic calls only</td>
</tr>
<tr>
<td></td>
<td></td>
<td>E1 QSIG</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>E1 R2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gateway Model</td>
<td>Supported Signaling Protocols</td>
<td>Trunk Interfaces</td>
<td>Port Types</td>
<td>Notes</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------------------------</td>
<td>------------------</td>
<td>--------------------------</td>
<td>------------------------------</td>
</tr>
<tr>
<td>MGCP</td>
<td>E1 PRI</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E1 QSIG</td>
<td></td>
<td></td>
<td></td>
<td>Supplementary Services</td>
</tr>
<tr>
<td>Cisco Catalyst 4000 Access Gateway Module (WS-X4604-GWY)</td>
<td>H.323</td>
<td>FXS</td>
<td>Loopstart or groundstart</td>
<td>Basic calls only</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FXO</td>
<td>Loopstart or groundstart</td>
<td></td>
</tr>
<tr>
<td>T1 CAS</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>T1/E1 QSIG</td>
<td></td>
<td></td>
<td></td>
<td>Basic calls only</td>
</tr>
<tr>
<td>T1/E1 PRI</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MGCP</td>
<td>FXS</td>
<td></td>
<td>Basic calls only</td>
<td></td>
</tr>
<tr>
<td></td>
<td>FXO</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>T1 CAS (E&amp;M)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>T1/E1 QSIG</td>
<td></td>
<td></td>
<td>Supplementary Services</td>
<td></td>
</tr>
<tr>
<td>T1/E1 PRI</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cisco Catalyst 4224 Voice Gateway Switch</td>
<td>H.323</td>
<td>FXS</td>
<td>Basic calls only</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>FXO</td>
<td></td>
<td></td>
</tr>
<tr>
<td>BRI</td>
<td>T1 CAS</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E1 R2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>T1/E1 QSIG</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>T1/E1 PRI</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| Cisco Catalyst 6000 8-Port Voice T1/E1 and Services Module (WS-X6608-T1) | MGCP | T1 CAS (E&M) | T1 PRI | T1 PRI

Note: The table provides a summary of supported signaling protocols, trunk interfaces, port types, and notes for various Cisco voice gateways.
### Gateways dial plans and route groups

Gateways use dial plans to access or call out to the PSTN, route groups, and group-specific gateways. The different gateways that are used within Cisco Unified Communications Solutions have dial plans that are configured in different places:

- Configure dial plan information for both Skinny and MGCP gateways in the Cisco Unified Communications Manager.
- Configure dial plans in Cisco Unified Communications Manager to access the H.323-based Cisco IOS software gateways. Configure dial peers in the H.323-based gateways to pass the call out of the gateway.

The route group points to one or more gateways and can choose the gateways for call routing based on preference. The route group can serve as a trunk group by directing all calls to the primary device and then using the secondary devices when the primary is unavailable. One or more route lists can point to the same route group.

All devices in a given route group share the same characteristics such as path and digit manipulation. Cisco Unified Communications Manager restricts the gateways that you can include in the same route group and the route groups that you can include in the same route list.

Route groups can perform digit manipulation that will override what was performed in the route pattern. Configuration information that is associated with the gateway defines how the call is actually placed and can override what was configured in the route pattern.

You can configure H.323 trunks, not H.323 gateways, to be gatekeeper-controlled trunks. This means that before a call is placed to an H.323 device, it must successfully query the gatekeeper.

Multiple clusters for inbound and outbound calls can share H.323 trunks, but MGCP and Skinny-based gateways remain dedicated to a single Cisco Unified Communications Manager cluster.

### Related Topics
- Configure gatekeeper and gatekeeper-controlled trunk, on page 67
- Route plan overview, on page 146

---

<table>
<thead>
<tr>
<th>Gateway Model</th>
<th>Supported Signaling Protocols</th>
<th>Trunk Interfaces</th>
<th>Port Types</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Catalyst 6000 8-Port Voice T1/E1 and Services Module (WS-X6608-E1)</td>
<td>MGCP</td>
<td>E1 PRI</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>E1 QSIG</td>
<td>Supplementary Services</td>
<td></td>
</tr>
<tr>
<td>Cisco Catalyst 6000 24-Port FXS Analog Interface Module (WS-X6624-FXS)</td>
<td>MGCP</td>
<td>FXS</td>
<td>Loopstart only</td>
<td>Basic calls only</td>
</tr>
</tbody>
</table>
Dependency records for gateways and their route groups and directory numbers

To find route groups or directory numbers that a specific gateway or gateway port is using, click the Dependency Records link that is provided on the Cisco Unified Communications Manager Administration Gateway Configuration window. The Dependency Records Summary window displays information about route groups and directory numbers that are using the gateway or port. To find out more information about the route group or directory number, click the route group or directory number, and the Dependency Records Details window displays. If the dependency records are not enabled for the system, the dependency records summary window displays a message.

Gateways and the Local Route Groups feature

A special virtual Local Route Group can be bound to a real route group differently based on the Local Route Group device pool setting of the originating device. Devices, such as phones, from different locales can therefore use identical route lists and route patterns, but Cisco Unified Communications Manager selects the correct gateway(s) for their local end.

If the Local Route Group feature is in use, configuration of gateways changes, particularly with respect to configuration of the following gateway fields:

- Called Party Transformation CSS
- Use Device Pool Called Party Transformation CSS

Gateways and the Calling Party Normalization feature

In line with E.164 standards, calling party normalization enhances the dialing capabilities of some phones and improves call back functionality when a call is routed to multiple geographical locations; that is, the feature ensures that the called party can return a call without needing to modify the directory number in the call log directories on the phone. Additionally, calling party normalization allows you to globalize and localize phone numbers, so the appropriate calling number presentation displays on the phone.

Configuring calling party normalization alleviates issues with toll bypass where the call is routed to multiple locations over the IP WAN. In addition, it allows Cisco Unified Communications Manager to distinguish the origin of the call to globalize or localize the calling party number for the phone user.

SIP trunks and MGCP gateways can support sending the international escape character, +, for calls. H.323 gateways/trunks do not support the + because the H.323 protocol does not support the international escape character, +. For outgoing calls through a gateway that supports +, Cisco Unified Communications Manager can send the + with the dialed digits to the gateway/trunk. For outgoing calls through a gateway/trunk that does not support +, the international escape character + gets stripped when Cisco Unified Communications Manager sends the call information to the gateway/trunk.

SIP does not support the number type, so calls through SIP trunks only support the Incoming Calling Party Unknown Number (prefix and digits-to-strip) settings.

You can configure the international escape character, +, to globalize the calling party number. For information on the international escape character, +, see Use the international escape character, on page 161.
Apply the international escape character to inbound calls over H.323 trunks

The H.323 protocol does not support the international escape character, +. To ensure that correct prefixes, including the international escape character, +, get applied for inbound calls over H.323 gateways/trunks, you must configure the incoming called party settings in the service parameter, device pool, H.323 gateway, or H.323 trunk windows; that is, configuring the incoming called party settings ensures that when a inbound call comes from a H.323 gateway or trunk, Cisco Unified Communications Manager transforms the called party number back to the value that was originally sent over the trunk/gateway.

For example, to ensure that the correct DN patterns get used with SAF/call control discovery for inbound calls over H.323 gateways/trunks, you must configure the incoming called party settings in the service parameter, device pool, or H.323 (non-gatekeeper controlled) trunk window. See the following example for more information.

- A caller places a call to +19721230000 to Cisco Unified Communications Manager A.
- Cisco Unified Communications Manager A receives +19721230000 and transforms the number to 55519721230000 before sending the call to the H.323 trunk. In this case, your configuration indicates that the international escape character + should be stripped and 555 should be prepended for calls of International type.
- For this inbound call from the trunk, Cisco Unified Communications Manager B receives 55519721230000 and transforms the number back to +19721230000 so that digit analysis can use the value as it was sent by the caller. In this case, your configuration for the incoming called party settings indicates that you want 555 to be stripped and +1 to be prepended to called party numbers of International type.

The service parameters support the Cisco CallManager service. To configure the service parameters, click Advanced in the Service Parameter Configuration window for the Cisco CallManager service; then, locate the H.323 pane for the following parameters:

- Incoming Called Party National Number Prefix - H.323
- Incoming Called Party International Number Prefix - H.323
- Incoming Called Party Subscriber Number Prefix - H.323
- Incoming Called Party Unknown Number Prefix - H.323

These service parameters allow you to prefix digits to the called number based on the Type of Number field for the inbound offered call. You can also strip a specific number of leading digits before the prefix gets applied. To prefix and strip digits by configuring these parameter fields, use the following formula, x:y, where x represents the exact prefix that you want to add to called number and y represents the number of digits stripped; be aware that the colon separates the prefix and the number of stripped digits. For example, enter 91010:6 in the field, which means that you want to strip 6 digits and then add 901010 to the beginning of the called number. In this example, a national call of 2145551234 becomes 910101234. You can strip up to 24 digits and prefix/add up to than 16 digits.

Gateway failover and fallback

This section describes how these Cisco voice gateways handle Cisco Unified Communications Manager failover and fallback situations.
MGCP gateways

To handle Cisco Unified Communications Manager failover situations, MGCP gateways receive a list of Cisco Unified Communications Managers that is arranged according to the Cisco Unified Communications Manager group and defined for the device pool that is assigned to the gateway. A Cisco Unified Communications Manager group can contain one, two, or three Cisco Unified Communications Managers that are listed in priority order for the gateway to use. If the primary Cisco Unified Communications Manager in the list fails, the secondary Cisco Unified Communications Manager gets used. If the primary and secondary Cisco Unified Communications Managers fail, the tertiary Cisco Unified Communications Manager gets used.

Fallback describes the process of recovering a higher priority Cisco Unified Communications Manager when a gateway fails over to a secondary or tertiary Cisco Unified Communications Manager. Cisco MGCP gateways periodically take status of higher priority Cisco Unified Communications Managers. When a higher priority Cisco Unified Communications Manager is ready, it gets marked as available again. The gateway reverts to the highest available Cisco Unified Communications Manager when all calls go idle or within 24 hours, whichever occurs first. The administrator can force a fallback either by stopping the lower priority Cisco Unified Communications Manager whereby calls get preserved, by restarting the gateway, which preserves calls, or by resetting Cisco Unified Communications Manager, which terminates calls.

Skinny Client Control Protocol (SCCP) gateways handle Cisco Unified Communications Manager redundancy, failover, and fallback in the same way as MGCP gateways.

IOS H.323 gateways

Cisco IOS gateways also handle Cisco Unified Communications Manager failover situations. By using several enhancements to the dial-peer and voice class commands in Cisco IOS Release 12.1(2)T, Cisco IOS gateways can support redundant Cisco Unified Communications Managers. The command, h225 tcp timeout seconds, specifies the time that it takes for the Cisco IOS gateway to establish an H.225 control connection for H.323 call setup. If the Cisco IOS gateway cannot establish an H.225 connection to the primary Cisco Unified Communications Manager, it tries a second Cisco Unified Communications Manager that is defined in another dial-peer statement. The Cisco IOS gateway shifts to the dial-peer statement with the next highest preference setting.

The following examples show the configuration for H.323 gateway failover:

```plaintext
interface FastEthernet0/0ip address 10.1.1.10 255.255.255.0
dial-peer voice 101 voip
destination-pattern 1111
session target ipv4:10.1.1.101
preference 0
voice class h323 1
dial-peer voice 102 voip
destination-pattern 1111
session target ipv4:10.1.1.102
preference 1
voice class h323 1
voice class h323 1
h225 timeout tcp establish 3
```
To simplify troubleshooting and firewall configurations, Cisco recommends that you use the new voip-gateway voip bind srcaddr command for forcing H.323 always to use a specific source IP address in call setup. Without this command, the source address that is used in the setup might vary and depends on protocol (RAS, H.225, H.245, or RTP).

---

**Note**

Cisco VG248 Analog Phone Gateway

The Cisco VG248 Analog Phone Gateway supports the Skinny Client Control Protocol (SCCP) for clustering and failover.

**Transfer calls between gateways**

Using Cisco Unified Communications Manager Administration, you can configure gateways as OnNet (internal) gateways or OffNet (external) gateways by using Gateway Configuration or by setting a clusterwide service parameter. Used in conjunction with the clusterwide service parameter, Block OffNet to OffNet Transfer, the configuration determines whether calls can be transferred over a gateway.

To use the same gateway to route both OnNet and OffNet calls, associate the gateway with two different route patterns. Make one gateway OnNet and the other OffNet with both having the Allow Device Override check box unchecked.

**Transfer capabilities using gateway configuration**

Using Cisco Unified Communications Manager Administration Gateway Configuration, you can configure a gateway as OffNet or OnNet. The system considers the calls that come to the network through that gateway OffNet or OnNet, respectively. Use the Gateway Configuration window field, Call Classification, to configure the gateway as OffNet, OnNet, or Use System Default. See the table below for description of these settings.

The Route Pattern Configuration window provides a drop-down list box called Call Classification, which allows you to configure a route pattern as OffNet or OnNet. When Call Classification is set to OffNet and the Allow Device Override check box is unchecked, the system considers the outgoing calls that use this route pattern as OffNet (if configured as OnNet and check box is unchecked, then outgoing calls are considered OnNet).

You can use the same gateway to route both OnNet and OffNet calls by associating the gateway with two different route patterns: one OnNet and the other OffNet, with both having the Allow Device Override check box unchecked. For outgoing calls, the outgoing device setting classifies the call as either OnNet or OffNet by determining whether the Allow Device Override check box is checked.

In route pattern configuration, if the Call Classification is set as OnNet, the Allow Device Override check box is checked, and the route pattern is associated with an OffNet gateway, the system considers the outgoing call OffNet.
Table 30: Gateway Configuration Call Classification Settings

<table>
<thead>
<tr>
<th>Setting Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OffNet</td>
<td>This setting identifies the gateway as being an external gateway. When a call comes in from a gateway that is configured as OffNet, the outside ring gets sent to the destination device.</td>
</tr>
<tr>
<td>OnNet</td>
<td>This setting identifies the gateway as being an internal gateway. When a call comes in from a gateway that is configured as OnNet, the inside ring gets sent to the destination device.</td>
</tr>
<tr>
<td>Use System Default</td>
<td>This setting uses the Cisco Unified Communications Manager clusterwide service parameter Call Classification.</td>
</tr>
</tbody>
</table>

Set up transfer capabilities by using Call Classification service parameter

To configure all gateways to be OffNet (external) or OnNet (internal), perform the following two steps:

**Procedure**

**Step 1**
Use the Cisco Unified Communications Manager clusterwide service parameter Call Classification.

**Step 2**
Configure individual gateways to Use System Default in the Call Classification field that is on the Gateway Configuration window.

Block transfer capabilities by using service parameters

Block transfer provides a way of restricting transfer between external devices, so fraudulent activity gets prevented. You can configure the following devices as OnNet (internal) or OffNet (external) to Cisco Unified Communications Manager:

- H.323 gateway
- MGCP FXO trunk
- MGCP T1/E1 trunk
- Intercluster trunk
- SIP trunk

If you do not want OffNet calls to be transferred to an external device (one that is configured as OffNet), set the Cisco Unified Communications Manager clusterwide service parameter, Block OffNet to OffNet Transfer, to True.

If a user tries to transfer a call on an OffNet gateway that is configured as blocked, a message displays on the user phone to indicate that the call cannot be transferred.
H.235 support for gateways

This feature allows Cisco Unified Communications Manager gateways to transparently pass through the shared secret (Diffie-Hellman key) and other H.235 data between two H.235 endpoints so that the two endpoints can establish a secure media channel.
IP telephony protocols

This chapter provides information about some of the different protocols and their interaction with Cisco Unified Communications Manager.

- IP protocols, page 381
- Analog telephony protocols, page 383
- Digital telephony protocols, page 385

IP protocols

Cisco Unified Communications Manager performs signaling and call control tasks such as digit analysis, routing, and circuit selection within the PSTN gateway infrastructure. To perform these functions, Cisco Unified Communications Manager uses industry standard IP protocols including H.323, MGCP, SCCP, and SIP. Use of Cisco Unified Communications Manager and these protocols gives service providers the capability to seamlessly route voice and data calls between the PSTN and packet networks.

H.323 Protocol

The International Telecommunications Union (ITU) developed the H.323 standard for multimedia communications over packet networks. As such, the H.323 protocol represents a proven ITU standard and provides multivendor interoperability. The H.323 protocol specifies all aspects of multimedia application services, signaling, and session control over an underlying packet network. Although audio is standard on H.323 networks, you can scale networks to include both video and data. You can implement the H.323 protocol in large enterprise networks, or you can deploy it over an existing infrastructure, which makes H.323 an affordable solution.

The basic components of the H.323 protocol comprise terminals, gateways, and gatekeepers (which provide call control to H.323 endpoints). Similar to other protocols, H.323 applies to point-to-point or multipoint sessions. However, compared to MGCP, H.323 requires more configuration on the gateway.

Related Topics

- Media Gateway Control Protocol (MGCP), on page 382
- Session Initiation Protocol (SIP), on page 382
- Skinny Client Control Protocol (SCCP), on page 382
**Media Gateway Control Protocol (MGCP)**

MGCP provides Cisco Unified Communications Manager with a powerful, flexible and scalable resource for call control. Cisco Unified Communications Manager uses MGCP to control media on the telephony interfaces of a remote gateway and also uses MGCP to deliver messages from a remote gateway to appropriate devices.

MGCP enables a call agent (media gateway controller) to remotely control and manage voice and data communication devices at the edge of multiservice IP packet networks. Because of its centralized architecture, MGCP simplifies the configuration and administration of voice gateways and supports multiple (redundant) call agents in a network. MGCP does not provide security mechanisms such as message encryption or authentication.

Using MGCP, Cisco Unified Communications Manager controls call processing and routing and provides supplementary services to the gateway. The MGCP gateway provides call preservation (the gateway maintains calls during failover and fallback), redundancy, dial-plan simplification (the gateway requires no dial-peer configuration), hookflash transfer, and tone on hold. MGCP-controlled gateways do not require a media termination point (MTP) to enable supplementary services such as hold, transfer, call pickup, and call park. If the MGCP gateway loses contact with its Cisco Unified Communications Manager, it falls back to using H.323 control to support basic call handling of FXS, FXO, T1 CAS, and T1/E1 PRI interfaces.

**Related Topics**
- H.323 Protocol, on page 381
- Skinny Client Control Protocol (SCCP), on page 382
- Session Initiation Protocol (SIP), on page 382

**Skinny Client Control Protocol (SCCP)**

SCCP uses Cisco-proprietary messages to communicate between IP devices and Cisco Unified Communications Manager. SCCP easily coexists in a multiple protocol environment. The Cisco Unified IP Phone represents an example of a device that registers and communicates with Cisco Unified Communications Manager as an SCCP client. During registration, a Cisco Unified IP Phone receives its line and all other configurations from Cisco Unified Communications Manager. After it registers, the system notifies it of new incoming calls, and it can make outgoing calls. The SCCP gets used for VoIP call signaling and enhanced features such as Message Waiting Indication (MWI).

The Cisco VG248 gateway represents another example of a device that registers and communicates with Cisco Unified Communications Manager by using SCCP.

**Related Topics**
- Media Gateway Control Protocol (MGCP), on page 382
- H.323 Protocol, on page 381
- Session Initiation Protocol (SIP), on page 382

**Session Initiation Protocol (SIP)**

The Internet Engineering Task Force (IETF) developed the SIP standard for multimedia calls over IP. ASCII-based SIP works in client/server relationships as well as in peer-to-peer relationships. SIP uses requests and responses to establish, maintain, and terminate calls (or sessions) between two or more end points. See the Session Initiation Protocol, on page 397 chapter for more information on SIP and the interaction between SIP and Cisco Unified Communications Manager.
Analog telephony protocols

Analog telephony signaling, the original signaling protocol, provides the method for connecting or disconnecting calls on analog trunks. By using direct current (DC) over two-wire or four-wire circuits to signal on-hook and off-hook conditions, each analog trunk connects analog endpoints or devices such as a PBX or analog phone.

To provide connections to legacy analog central offices and PBXs, Cisco Unified Communications Manager uses analog signaling protocols over analog trunks that connect voice gateways to analog endpoints and devices. Cisco Unified Communications Manager supports these types of analog trunk interfaces:

- **Foreign Exchange Office (FXO)**- Analog trunks that connect a gateway to a central office (CO) or private branch exchange (PBX).
- **Foreign Exchange Station (FXS)**- Analog trunks that connect a gateway to plain old telephone service (POTS) device such as analog phones, fax machines, and legacy voice-messaging systems.

You can configure loop-start, ground-start, or E&M signaling protocols for FXO and FXS trunk interfaces depending on the gateway model that is selected. You must use the same type of signaling on both ends of the trunk interface to ensure that the calls properly connect.

**Loop-Start Signaling**

Loop-start signaling sends an off-hook signal that starts a call and an on-hook signal that opens the loop to end the call. Loop-start trunks lack positive disconnect supervision, and users can experience glare when two calls seize the trunk at the same time.

**Related Topics**

- E1 CAS, on page 385
- Ground-Start Signaling, on page 383
- E&M Signaling, on page 384
- Channel Associated Signaling (CAS), on page 384

**Ground-Start Signaling**

Ground-start signaling provides current detection mechanisms at both ends of the trunk to detect off-hook signals. This mechanism permits endpoints to agree on which end is seizing the trunk before it is seized and minimizes the chance of glare. Ground start provides positive recognition of connects and disconnects and is the preferred signaling method for PBX connections. Some PBXs do not support ground-start signaling, so you must use loop-start signaling for the trunk interface.

**Related Topics**

- E1 CAS, on page 385
- E&M Signaling, on page 384
E&M Signaling

E&M signaling uses direct current (DC) over two-wire or four-wire circuits to signal to the endpoint or CO switch when a call is in receive or transmit (E&M) state. E&M signaling uses signals that indicate off-hook and on-hook conditions. When the connection is established, the audio transmission occurs. Ensure that the E&M signaling type is the same for both ends of the trunk interface. For successful connections, Cisco Unified Communications Manager supports these types of E&M signaling:

Wink-start signaling

The originating side sends an off-hook signal and waits to receive a wink pulse signal that indicates the receiving end is ready to receive the dialed digits for the call. Wink start represents the preferred signaling method because it provides answer supervision. Not all COs and PBXs support wink-start signaling.

Delay-dial signaling

The originating side sends an off-hook signal, waits for a configurable time, and then checks whether the receiving end is on hook. The originating side sends dialed digits when the receiving side is on hook. The delay allows the receiving end to signal when it is ready to receive the call.

Immediate-start signaling

The originating side goes off hook, waits for a finite time (for example 200 ms), and then sends the dial digits without a ready signal from the receiving end.

Related Topics

- E1 CAS, on page 385
- Channel Associated Signaling (CAS), on page 384
- Ground-Start Signaling, on page 383
- Loop-Start Signaling, on page 383

Channel Associated Signaling (CAS)

Channel associated signaling (CAS) sends the on hook and off hook signals as bits within the frames on the same channel as the audio transmission. CAS gets often referred to as robbed bit signaling because CAS takes bits from the voice channel for signaling. These signals can include supervision, addressing, and tones such as busy tone or dial tone.

You can use T1 CAS and E1 CAS digital trunk interfaces to connect a Cisco Unified Communications Manager call to a CO, a PBX, or other analog device.

Related Topics

- E&M Signaling, on page 384
- Ground-Start Signaling, on page 383
- Loop-Start Signaling, on page 383
T1 CAS

The T1 CAS trunk interface uses in-band E&M signaling to carry up to 24 connections on a link. Both ends of the T1 link must specify T1 CAS signaling. Cisco Unified Communications Manager provides the T1 CAS signaling option when you configure ports on some MGCP and H.323 voice gateways and network modules. For more information about supported gateways, see the Voice gateway model summary, on page 365.

E1 CAS

Some Cisco gateways in H.323 mode can support the E1 CAS trunk interface that provides up to 32 connections on the link. You must configure the E1 CAS signaling interface on the gateway, not in Cisco Unified Communications Manager Administration. Both ends of the E1 link must specify E1 CAS signaling. For a list of H.323 gateways that support E1 CAS, see the Voice gateway model summary, on page 365. See documentation for the specific gateway for configuration information.

Related Topics

- Loop-Start Signaling, on page 383
- Ground-Start Signaling, on page 383
- E&M Signaling, on page 384

Digital telephony protocols

Digital telephony protocols use common channel signaling (CCS), a dedicated channel that carries only signals. In a T1 link, one channel carries the signals while the other channels carry voice or data. The latest generation of CCS, known as Signaling System 7 (SS7), provides supervision, addressing, tones, and a variety of services such as automatic number identification (ANI).

Integrated Services Digital Network (ISDN) specifies a set of international standards for user access to private or public network services. ISDN provides both circuit-based and packet-based communications to users.

Basic Rate Interface (BRI)

Basic rate interface (BRI), which is used for small office and home communications links, provides two B-channels for voice and data and one D-channel for signaling.

Related Topics

- T1 Primary Rate Interface (T1 PRI), on page 385
- E1 Primary Rate Interface (E1 PRI), on page 386
- Q.Signaling (QSIG), on page 386
- QSIG interface to Cisco Unified Communications Manager, on page 395

T1 Primary Rate Interface (T1 PRI)

Corporate communications links in North America and Japan use the T1 primary rate interface (PRI). T1 PRI provides 23 B-channels for voice and data and one D-channel for common channel signaling. T1 PRI uses a communication rate of 1.544 Mb/s.
E1 Primary Rate Interface (E1 PRI)

Corporate communications in Europe use the E1 PRI primary rate interface (PRI). E1 PRI provides 30 B-channels for voice and data, one D-channel for common signaling, and one framing channel. E1 PRI uses a rate of 2.048 Mb/s.

Q.Signaling (QSIG)

Because enterprises maintain existing telecommunication equipment from a variety of vendors, the protocol system, Q signaling (QSIG), provides interoperability and feature transparency among a variety of telecommunications equipment.

The QSIG protocol, a series of international standards, defines services and signaling protocols for Private Integrated Services Networks (PISNs). These standards use Integrated Services Digital Networks (ISDN) concepts and conform to the framework of International Standards for Open Systems Interconnection as defined by ISO/IEC. The QSIG protocol acts as a variant of ISDN D-channel voice signaling. The ISDN Q.921 and Q.931 standards provides the basis for QSIG protocol, which sets worldwide standard for PBX interconnection.

The QSIG protocol enables Cisco voice switching services to connect to PBXs and key systems that communicate by using QSIG protocol. For QSIG basic call setup, Cisco devices can route incoming voice calls from a private integrated services network exchange (PINX) device across a WAN to a peer Cisco device that can transport the signaling and voice packets to another PINX device, which are PBXs, key systems, or Cisco Unified Communications Manager servers that support QSIG protocol.

In a basic QSIG call, a user in a PINX can place a call to a user that is in a remote PINX. The called party receives the caller name or number as the call rings. The calling party receives the called name and number when the user phone rings in the remote PINX. All the features that are available as a PBX user operate transparently across the network. QSIG protocol provides supplementary and additional network features, as defined for PISNs, if both ends of the call support the corresponding set of QSIG features.

To make supplementary features available to network users, ensure that all PBXs in the network support the same feature set.

Cisco tested Cisco Unified Communications Manager QSIG feature functionality with the following PBX vendors: Lucent/Avaya Definity G3R using T1 or E1, Avaya MultiVantage and Communication Manager, Alcatel 4400 using E1 or T1, Ericsson MD110 using E1, Nortel Meridian using E1 or T1, Siemens Hicom 300 E CS using T1, Siemens Hicom 300 E using E1, and Siemens HiPath 4000.
Annex M.1 (message tunneling for QSIG)

The Annex M.1 feature uses intercluster trunks and H.225 trunks to transport (tunnel) non-H.323 protocol information in H.323 signaling messages between Cisco Unified Communications Managers. Annex M.1 supports QSIG calls and QSIG call independent signaling connections. After you complete intercluster trunk configuration in Cisco Unified Communications Manager Administration, QSIG tunneling supports the following features: Call Completion, Call Diversion, Call Transfer, Identification Services, Message Waiting Indication, and Path Replacement.

Note

For designated third-party switch equipment, the Annex M.1 feature can also use H.323 gateways to transport (tunnel) non-H.323 protocol information in H.323 signaling messages between Cisco Unified Communications Managers. See the Cisco Unified Communications Manager Software Compatibility Matrix for information about Annex M.1 feature interoperability with third-party vendors.

Tip

If you use a gatekeeper, you must configure every gateway in the network for QSIG tunneling. If any gateway in the network does not support QSIG tunneling, calls drop at the intercluster trunk that is configured for QSIG tunneling.

For Cisco Unified Communications Manager to support QSIG tunneling, you must choose the QSIG option in the Tunneled Protocol drop-down list box and check the Path Replacement Support check box in the Trunk Configuration window in Cisco Unified Communications Manager Administration. By default, Cisco Unified Communications Manager sets the option in the Tunneled Protocol drop-down list box to None; after you configure the QSIG Tunneled Protocol option, the Path Replacement Support check box automatically becomes checked. If you do not require path replacement over Annex M.1 or QSIG-tunneled trunks, you can uncheck the check box.

When you set the Tunneled Protocol field to None, Cisco Unified Communications Manager automatically grays out the Path Replacement Support check box. When you set the Tunneled Protocol field to QSIG, you cannot configure the Redirecting Number IE Delivery (Inbound), Redirecting Number IE Delivery (Outbound), or Display IE Delivery options.

Tip

Cisco Unified Communications Manager does not support protocol profile 0x91 ROSE encoding with Annex M.1.

QSIG tunneling over SIP trunk

In a call-processing environment that uses Session Initiation Protocol (SIP), you can use SIP trunks to configure a signaling interface with Cisco Unified Communications Manager for SIP calls. SIP trunks (or signaling interfaces) connect Cisco Unified Communications Manager clusters with a SIP proxy server. The SIP signaling interface uses requests and responses to establish, maintain, and terminate calls (or sessions) between two or
more endpoints. For more information about SIP and configuring SIP trunks, see the SIP and Cisco Unified Communications Manager, on page 398.

Cisco Unified Communications Manager supports QSIG tunneling over a SIP trunk. QSIG tunneling supports the following features: Call Back, Call Completion, Call Diversion, Call Transfer, Identification Services, Message Waiting Indication, and Path Replacement.

**Note**

Cisco Unified Communications Manager supports only connection retention mode for Call Back on an Cisco Intercompany Media Engine (IME) trunk. For information about Cisco IME, see the Cisco Intercompany Media Engine Installation and Configuration Guide.

For Cisco Unified Communications Manager to support QSIG tunneling over a SIP trunk, you must choose the QSIG option in the Tunneled Protocol drop-down list box and check the Path Replacement Support check box in the Trunk Configuration window in Cisco Unified Communications Manager Administration. By default, Cisco Unified Communications Manager sets the option in the Tunneled Protocol drop-down list box to None; after you configure the QSIG Tunneled Protocol option, the Path Replacement Support check box automatically becomes checked. If you do not require path replacement over Annex M.1 or QSIG-tunneled trunks, you can uncheck the check box.

**Note**

When you create a SIP trunk with Cisco Intercompany Media Engine selected as the trunk service type, the default for the Tunneled Protocol field is QSIG. QSIG must be the tunneled protocol for QSIG features to work on a Cisco IME trunk.

**Tip**

Resetting a trunk drops any calls in progress that are using that trunk. Restarting a gateway tries to preserve the calls in progress that are using that gateway, if possible. Other devices wait until calls complete before restarting or resetting. Resetting or restarting an H.323 or SIP device does not physically reset or restart the hardware; resetting or restarting only reinitializes the configuration that Cisco Unified Communications Manager loads.

For SIP trunks, Restart and Reset behave the same way, so all active calls disconnect when either action is taken. Trunks do not have to undergo a Restart or Reset when Packet Capture is enabled or disabled.

**Note**

Remote-Party-ID (RPID) headers coming in from the SIP gateway can interfere with QSIG content and cause unexpected behavior with Call Back capabilities. To prevent interference with the QSIG content, turn off the RPID headers on the SIP gateway.

To turn off RPID headers on the SIP gateway, apply a SIP profile to the voIP dial peer on the gateway, as shown in the following example:

```plaintext
voice class sip-profiles 1000
request ANY sip-header Remote-Party_ID remove
response ANY sip-header Remote-Party-ID remove
dial-peer voice 124 voip
destination-pattern 3...
signaling forward unconditional
session protocol sipv2
```
Basic call for QSIG

QSIG basic call setup provides the dynamic establishment of voice connections from an originating PINX (PBX or Cisco Unified Communications Manager) across a private network or virtual private network (VPN) to another PINX. You must use digital T1 or E1 primary rate interface (PRI) trunks to support QSIG protocol.

Call completion

The following Call Completion services, which rely on the Facility Selection and Reservation feature, provide Cisco Call Back functionality over QSIG-enabled trunks:

- Completion of Calls to Busy Subscribers (CCBS)-When a calling party receives a busy tone, the caller can request that the call complete when the busy destination hangs up the phone and becomes available.

- Completion of Calls on No Reply (CCNR)-When a calling party receives no answer at the destination, the calling party can request that the call complete after the activity occurs on the phone of the called party.

Cisco Unified Communications Manager and the Call Completion services use the CallBack softkey on supported Cisco Unified IP Phone 7940, 7960, and 7970 in a Cisco Unified Communications Manager cluster or over QSIG trunks. Likewise, the following devices support QSIG Call Completion services:

- Cisco Unified IP Phone 7905, 7910, 7912, 7940, 7960, 7970
- Cisco VGC Phone, Cisco IP Communicator, and Cisco Phone that is running SCCP
- CTI route point that forwards calls to supported devices

The Callback Calling Search Space service parameter, which works with the Cisco CallManager service, allows an originating PINX to route a call setup request to a CTI device that exists on the terminating PINX. This functionality supports CTI applications, such as Cisco Unified Communications Manager Assistant. For more information on this service parameter, click the ? that displays in the upper corner of the Service Parameter window.

- QSIG trunks

In addition to configuring the Cisco Call Back feature in Cisco Unified Communications Manager Administration, as described in the SIP and Cisco Unified Communications Manager, on page 398 chapter of the Cisco Unified Communications Manager Features and Services Guide, you may need to update the default settings for the Cisco Call Back service parameters; that is, if the Cisco Technical Assistance Center (TAC) directs you to do so. Cisco Call Back service parameters include Connection Proposal Type, Connection Response Type, Callback Request Protection Timer, Callback Recall Timer, and Callback Calling Search Space. For information on these parameters, click the ? that displays in the upper corner of the Service Parameter window.

Call diversion

Cisco Unified Communications Manager supports call diversion by rerouting and call diversion by forward switching. When call diversion by rerouting occurs, the originating PINX receives a request from the receiver of the call to divert the call to another user. The system creates a new call between the originator and the diverted-to user, and an additional CDR gets generated.
In Cisco Unified Communications Manager Administration, the Cisco CallManager service uses the following parameters to perform call diversion by rerouting: Call Diversion by Reroute Enabled and Call Reroute T1 Timer. If you want to use call diversion by rerouting, you must set the service parameters to the values that are specified in the `?` help, which displays when you click the `?` in the upper corner of the Service Parameter window. If you do not configure the service parameters, call diversion by forward switching automatically occurs.

Cisco Unified Communications Manager cannot request that the originating PINX divert the call, but Cisco Unified Communications Manager can validate the directory number to which the call is diverted by terminating restriction QSIG messages. Call diversion by rerouting does not support non-QSIG trunks. If you do not use a uniform dial plan for your network, use call diversion by forward switching and path replacement to optimize the path between the originating and terminating users.

If the receiver of the incoming call and the diverted-to user exist in the same PINX, Cisco Unified Communications Manager uses call diversion by forward switching. If call diversion by rerouting is not successful for any reason, for example, the rerouting timer expires, forward switching occurs.

QSIG diversion supplementary services provide call-forwarding capabilities that are similar to familiar Cisco Unified Communications Manager call-forwarding features, as indicated in the following list:

- Call Forward All (CFA) configuration supports Call Forwarding Unconditional (SS-CFU).
- Call Forward Busy (CFB) configuration supports Call Forwarding Busy (SS-CFB).
- Call Forward No Answer (CFNA) configuration supports Call Forwarding No Reply (SS-CFNR).
- Cisco Unified Communications Manager does not support Call Deflection (SS-CD).

To provide feature transparency with other PBXs in the network, the system passes information about a forwarded call during the call setup and connection over QSIG trunks. Phone displays can present calling name/number, original called name/number, and last redirecting name/number information to show the destination of the forwarded call. Call identification restrictions can impact what displays on the phone. See the Identification services, on page 392 for more information.

QSIG supplementary services can provide the information to place the voice message from a diverted call into the originally called party voice mailbox. Be aware that voice-mail configuration may override call-forwarding configuration settings.

Cisco Unified Communications Manager does not invoke call diversion by rerouting when the system forwards the call to the voice mailbox. If the connection to the voice mail server occurs over a QSIG trunk and you want to use call diversion by rerouting, you must enter the voice mail pilot number in the appropriate Destination field instead of checking the Voice Mail check box in the Directory Number Configuration window.

---

**Tip**

When calls are forwarded among multiple PINXs, a forwarding loop can result. To avoid calls being caught in a looping condition, or entering a long forwarding chain, configure the Forward Maximum Hop Count service parameter for the Cisco CallManager service. Setting this service parameter above 15 makes your QSIG configuration noncompliant with international standards.

---

**Call transfer**

Cisco Unified Communications Manager supports call transfer by join only.
When a user transfers a call to another user, the QSIG identification service changes the connected name and number that displays on the transferred party phone. Call identification restrictions can impact what displays on the phone.

The call transfer supplementary service interacts with the path replacement feature to optimize the trunk connections when a call transfers to a caller in another PINX. For more information about path replacement, see the Path replacement, on page 394.

Compatibility with older versions of QSIG Protocol (ECMA)

To create Cisco Unified Communications Manager compatibility with your version of the QSIG protocol, configure the ASN.1 ROSE OID Encoding and QSIG Variant service parameters.

Tip
For more information on these parameters, click the ? that displays in the upper corner of the Service Parameter window.

If you choose ECMA for the QSIG Variant parameter, you must choose the Use Global Value (ECMA) setting for the ASN.1 ROSE OID Encoding service parameter.

If you choose ISO for the QSIG Variant parameter, you normally choose the Use Local Value setting for the ASN.1 ROSE OID Encoding service parameter. You may need other configurations in unusual situations.

Cisco Unified Communications Manager supports using Annex M.1 to tunnel QSIG over intercluster trunks. To configure Annex M.1, do one of the following:

• Set the ASN.1 ROSE OID Encoding to Use Local Value and the QSIG Variant to ISO (Protocol Profile 0x9F).
• Set the ASN.1 ROSE OID Encoding to Use Global Value (ECMA) and the QSIG Variant to ECMA.

Note
You can also configure the ASN.1 ROSE OID Encoding and QSIG Variant parameters for an individual gateway or trunk.

Facility selection and reservation

The facility selection and reservation feature allows you to make calls by using mixed route lists, which contain route groups that use different protocols. This feature supports mixed route lists, which include the following types of facilities:

• E1 or T1 PRI trunks that use the QSIG protocol
• E1 or T1 PRI trunks that use a protocol other than QSIG
• T1-CAS gateways
• FXO ports
• Intercluster trunks
You cannot add route groups with H.323 gateways to a route list that includes QSIG route groups.

When you configure the route list, configure the QSIG route groups as the first choice, followed by the non-QSIG route groups that serve as alternate connections to the PSTN. Make sure that you include additional route groups for QSIG calls in addition to the private network QSIG facilities. When no QSIG trunks are available for a call, you want to provide alternate routes over the PSTN for calls.

If a call requires a QSIG facility, Cisco Unified Communications Manager hunts through the route groups to reserve the first available QSIG facility. If a QSIG facility is unavailable, Cisco Unified Communications Manager uses a non-QSIG facility to failover to the PSTN.

If a call does not require a QSIG facility, Cisco Unified Communications Manager hunts through the route groups to find the first available facility.

The Path Replacement, Message Waiting Indication, and Call Completion supplementary services require a QSIG facility to meet QSIG signaling compliance requirements. If a QSIG facility is not available for one of the aforementioned services, the call does not meet QSIG signaling compliance requirements, and the feature fails.

Identification services

When a call alerts and connects to a PINX, identification services can display the caller name/ID on a phone in the terminating PINX, and, likewise, the connected party name/ID on a phone in the originating PINX. QSIG identification restrictions allow you to control the presentation or display of this information between Cisco Unified Communications Manager and the connected PINX.

Supported supplementary services apply on a per-call basis, and presentation settings for call identification information are set at both ends of the call. Cisco Unified Communications Manager provides configuration settings to control the following caller identification number (CLID) and caller name (CNAM) information on phone displays:

- **Calling Line Identification Presentation/Restriction-** Displays the calling number (CLIP) or restricts the display of the calling number (CLIR).
- **Calling Name Identification Presentation/Restriction-** Displays the calling name (CNIP) or restricts the display of the calling name (CNIR).
- **Connected Line Identification Presentation/Restriction-** Displays the number of the connected line (COLP) or restricts the display of the connected line (COLR).
- **Connected Name Identification Presentation/Restriction-** Displays the name of the connected party (CONP) or restricts the display of the connected name (CONR).

Configuration settings for the outgoing call get sent to the terminating PINX, where the settings may get overwritten. The connected line and name configuration gets set on the terminating side of the call; after the originating PINX receives the configuration settings, the originating PINX may override the configuration.

**Tip**

When you restrict a name, the display shows “Private,” and the display remains blank for a restricted calling line number.

You can allow or restrict display information for all calls by configuring fields in the Gateway Configuration window, or you can control display information on a call-by-call basis by using fields in the Route Patterns...
and Translation Patterns windows. The presentation setting for the gateway overrides the setting for the route pattern. Translation pattern presentation settings override route pattern presentation settings.

Cisco Unified Communications Manager supports “Alerting on ring” only, and the QSIG Alerting Name that you configure allows you to send and receive call name information while the phone rings. In the Directory Number Configuration window in Cisco Unified Communications Manager Administration, you configure the Alerting Name field for shared and nonshared directory numbers. When two phones ring for the shared directory number, the name that you entered in the Alerting Name field displays on the phone of the called party at the terminating PINX, unless translation pattern restrictions affect the information that displays. Route pattern restrictions may affect the information that displays on caller phone at the originating PINX.

Tip

You configure Alerting Name identification restrictions by setting the Connected Name configuration parameters.

If you do not configure an Alerting Name, only the directory number displays on the calling party phone when alerting occurs. If you configure a Display Name that is configured for the called party, the Display Name displays on the calling party phone when the call connects. If you do not enter a Display Name or an Alerting Name, no name displays on the calling party phone during the call. You cannot use Alerting Name with the following device types:

- PRI trunks
- FXS/FXO ports for MGCP gateways
- MGCP T1-CAS gateways

The Transmit UTF-8 Names in QSIG APDU check box in Cisco Unified Communications Manager Administration uses the user locale setting of the device pool to determine whether to send unicode and whether to translate received Unicode information.

For the sending device, if you check this check box and the user locale setting in the device pool matches the terminating phone user locale, the device sends unicode and encodes in UTF-8 format. If the user locale settings do not match, the device sends ASCII and encodes in UTF-8 format.

If the configuration parameter is not set and the user locale setting in the device pool matches the terminating phone user locale, the device sends unicode (if the name uses 8-bit format) and encodes in ISO8859-1 format.

Message Waiting Indication (MWI) service

In a QSIG network, when a PINX includes a connected voice-messaging system that services users in another PINX, the message center PINX can send the following message waiting indication (MWI) signals to the other PINX:

- MWI Activate-Send a signal to another PINX to activate MWI on the served user phone after the voice-messaging system receives a message for that phone.
- MWI De-activate-Send a signal to deactivate the MWI after the user receives messages in the associated voice-messaging system.

Note

Cisco Unified Communications Manager does not support the MWI interrogation service.

A PINX that is not a message center can receive MWI signals and perform the following tasks:
• MWI Activate-Receive a signal from another PINX to activate MWI on the served user phone.

• MWI De-activate-Receive a signal to deactivate the MWI on the served user phone.

If the voice-messaging system connects to Cisco Unified Communications Manager by using QSIG connections or by using the Cisco Messaging Interface (CMI), the message waiting indicators get set based on QSIG directives.

When a call is forwarded to a number and then diverted to a voice-messaging system, QSIG supplementary services can provide the information to place the voice message in the originally called party voice mailbox.

The Message Waiting Indication service, which uses the existing dial number for message waiting that is set up in Cisco Unified Communications Manager Administration, does not require any additional configuration.

Path replacement

In a QSIG network, after a call is transferred or forwarded to a phone in a third PINX, multiple connections through several PINX(s) can exist for the call. After the call connects, the path replacement feature drops the connection to the transit PINX(s) and creates a new call connection to the terminating PINX.

![Note](image)

Cisco Unified Communications Manager provides “requesting” and “cooperating” PINX messages only. If configured for QSIG, Cisco Unified Communications Manager responds to third-party vendor PINX “inviting” messages, although Cisco Unified Communications Manager will not originate “inviting” messages.

Cisco Unified Communications Manager does not support path retention.

Cisco Unified Communications Manager initiates path replacement for calls that are transferred by joining and for calls that are diverted by forward switching only. Calls that involve multiple trunks, for example, conference calls, do not use path replacement; however, if you choose the QSIG option for the Tunneled Protocol drop-down list box and check the Path Replacement Support check box for gatekeeper-controlled or non-gatekeeper-controlled intercluster trunks, path replacement occurs over the intercluster trunk and the other QSIG intercluster or PRI trunk that is used to transfer or divert the call.

When you use CTI applications with path replacement, the leg of the call that uses path replacement has a different Global Caller ID than the originating leg of the call. After a call is forwarded or transferred, if the remaining parties use the same Cisco Unified Communications Manager, two Global Caller IDs exist, one for each party. The system deletes one of the Global Caller IDs, both parties in the call have the same Global Caller ID.

![Tip](image)

This section provides information on a few path replacement service parameters. For a complete list of service parameters and for detailed information on the parameters, click the ? that displays in the upper corner of the Service Parameter Configuration window.

Because the QSIG protocol passes the extension number or directory number but does not pass translated or inserted numbers, use QSIG features, such as path replacement, in a network with a uniform dial plan. When a private network uses nonunique directory numbers in the dial plan, you must reroute calls through a PINX ID, which is a unique directory number for every PINX in the network. The path replacement feature uses the PINX ID, if configured, instead of the called or calling party number that the Identification services, on page 392 describes. To configure the PINX ID, perform the following tasks in Cisco Unified Communications Manager Administration:
• Configure the PINX ID service parameter(s) for the Path Replacement feature. (The Path Replacement feature uses the Cisco CallManager service.)

• Create a call pickup group that includes only the PINX ID.

Tip
Reserve the PINX ID call pickup group for PINX ID usage. Do not add other directory numbers to this call pickup group.

Cisco Unified Communications Manager provides the Path Replacement Calling Search Space service parameter, so you can configure the calling search space that the cooperating PINX uses to send the outbound SETUP message to the requesting PINX. If you do not specify a value for the Path Replacement Calling Search Space service parameter, the requesting PINX uses the calling search space of the end user that is involved in the call.

You configure Path Replacement settings in the Service Parameter window for the Cisco CallManager service. Path Replacement service parameters include Path Replacement Enabled, Path Replacement on Tromboned Trunks, Start Path Replacement Minimum Delay Time, Start Path Replacement Maximum Delay Time, Path Replacement PINX ID, Path Replacement Timers, Path Replacement Calling Search Space, and so on. To obtain information about these parameters, click the ? that displays in the Service Parameter window.

Path replacement performance counters allow you to track when path replacement occurs. For information on performance counters, see the Cisco Unified Serviceability Administration Guide.

For each call, the system generates more than one CDR for the path replacement feature. One CDR gets generated for the caller at the originating PINX; another CDR gets generated for the called party at the PINX where path replacement is initiated.

Note
When a Cisco IP Softphone user chooses to perform a consultive transfer to move a call to another PINX, path replacement can occur; if the user performs a direct (blind) transfer, path replacement cannot occur. For more information about Cisco IP Softphone, see the Cisco IP Softphone documentation that supports your version of the application.

QSIG interface to Cisco Unified Communications Manager

For Cisco Unified Communications Manager to support QSIG functionality, ensure that QSIG backhauls directly to Cisco Unified Communications Manager. Cisco Unified Communications Manager interconnects to a QSIG network by using an MGCP gateway and T1 or E1 PRI connections to the PISN. The MGCP gateway establishes the call connections. By using the PRI backhaul mechanism, the gateway passes the QSIG messages to Cisco Unified Communications Manager to enable setting up QSIG calls and sending QSIG messages to control features.

When a PBX connects to a gateway that is using QSIG via H.323, calls that occur between phones on the PBX and IP phones that are attached to the Cisco Unified Communications Manager can have only basic PRI functionality. The gateway that terminates the QSIG protocol provides only the Calling Line Identification (CLID) and Direct Inward Dialed (DID) number rather than Cisco Unified Communications Manager providing the information.

Related Topics

Basic Rate Interface (BRI), on page 385
T1 Primary Rate Interface (T1 PRI), on page 385
E1 Primary Rate Interface (E1 PRI), on page 386
CHAPTER 41

Session Initiation Protocol

This chapter provides information about Session Initiation Protocol (SIP) and the interaction between SIP and Cisco Unified Communications Manager.

- SIP trunk configuration, page 397
- SIP phone configuration, page 397
- SIP networks, page 398
- SIP and Cisco Unified Communications Manager, page 398
- SIP functions that are supported in Cisco Unified Communications Manager, page 410
- Cisco Unified Communications Manager SIP endpoints overview, page 438
- SIP line side overview, page 440
- SIP standards, page 440
- Cisco Unified Communications Manager functionality that is supported by phones that are running SIP, page 443

SIP trunk configuration

The Set up SIP trunk, on page 449 provides an overview of the steps that are required to configure SIP trunk in Cisco Unified Communications Manager, along with references to related procedures and topics.

SIP phone configuration

The Phone configuration, on page 460 provides an overview of the steps that are required to configure a Cisco Unified IP Phone that runs SIP.

If you want to configure a third-party phone that runs SIP, see the Cisco Unified Communications Manager Administration Guide.
SIP networks

A SIP network uses the following components:

- **SIP Proxy Server** - The proxy server works as an intermediate device that receives SIP requests from a client and then forwards the requests on the behalf of the client. Proxy servers can provide functions such as authentication, authorization, network access control, routing, reliable request retransmission, and security.

- **Redirect Server** - The redirect server provides the client with information about the next hop or hops that a message should take, and the client then contacts the next hop server or user agent server directly.

- **Registrar Server** - The registrar server processes requests from user agent clients for registration of their current location. Redirect or proxy servers often contain registrar servers.

- **User Agent (UA)** - UA comprises a combination of user agent client (UAC) and user agent server (UAS) that initiates and receives calls. A UAC initiates a SIP request. A UAS, a server application, contacts the user when it receives a SIP request. The UAS then responds on behalf of the user. Cisco Unified Communications Manager can act as both a server and a client (a back-to-back user agent).

SIP uses a request/response method to establish communications between various components in the network and to ultimately establish a call or session between two or more endpoints. A single session may involve several clients and servers.

Identification of users in a SIP network works through:

- A unique phone or extension number.

- A unique SIP address that appears similar to an e-mail address and uses the format `sip:<userID>@<domain>`. The user ID can comprise either a user name or an E.164 address. Cisco Unified Communications Manager only supports E.164 addresses; it does not support e-mail addresses.

- An e-mail address format (`employee@company.com`) that is supported on Cisco Unified Communications Manager with SIP route patterns.

**SIP and Cisco Unified Communications Manager**

All protocols require that either a signaling interface (trunk) or a gateway be created to accept and originate calls. For SIP, the user must configure a SIP trunk.

SIP trunks connect Cisco Unified Communications Manager networks and SIP networks that are served by a SIP proxy server, as the figure below demonstrates. As with other protocols, SIP components fit under the device layer of Cisco Unified Communications Manager architecture. As is true for the H.323 protocol, you can configure multiple logical SIP trunks in the Cisco Unified Communications Manager database and associate them with route groups, route lists, and route patterns. To provide redundancy, in the event of failure of one logical SIP interface, other logical SIP interfaces provide services in the same route group list. Assigning multiple Cisco Unified Communications Manager nodes under SIP trunk device pools also achieves redundancy.

SIP trunks can simultaneously run on all nodes and Cisco Unified Communications Manager can randomly choose from any of the available SIP trunks that can reach a given node. The system ensures that, over time and on average, all 16 nodes in the core cluster are used equally. This practice prevents system resources on some nodes from remaining idle while other nodes handle an unsustainable call burden.
Callback to external numbers is not supported on SIP ICTs.

Figure 39: SIP and Cisco Unified Communications Manager Interaction

SIP trunks support multiple port-based routing. Multiple SIP trunks on Cisco Unified Communications Manager can use port 5060, the default, which is configurable from the SIP Trunk Security Profile Configuration window. For TCP/UDP, SIP trunks use the remote host and local listening port to do the routing (the remote host can comprise IP, FQDN, or SRV). For TLS, SIP trunks use X.509 Subject Name to do the routing.

For SIP trunks, Cisco Unified Communications Manager only accepts calls from the SIP device whose IP address matches the destination address of the configured SIP trunk. In addition, the port on which the SIP message arrives must match the one that is configured on the SIP trunk. After the call is accepted, Cisco Unified Communications Manager uses the configuration for the SIP profile setting. Reroute Incoming Request to new Trunk based on, which is configured on the SIP trunk on which the call arrives, to determine whether the call gets rerouted to another SIP trunk. Depending on the configuration, Cisco Unified Communications Manager may perform one of the following tasks:

- Never reroute to a different SIP trunk.
- Parse the IP address or domain name and port number in the contact header and attempt to match the information to a SIP trunk; if a SIP trunk is found, reroute the call. If no SIP trunk is found, the SIP trunk on which the call arrived handles the call.
- Parse the IP address or domain name and port number in the Call-Info header, look for the parameter, purpose=x-cisco-origIP, and attempt to match the IP address and port to a SIP trunk; if a SIP trunk is found, reroute the call. If no SIP trunk is found or if the parameter does not exist in the Call-Info header, the SIP trunk on which the call arrived handles the call.

Related Topics

SIP trunk, on page 453

Media Termination Point (MTP) devices

You can configure Cisco Unified Communications Manager SIP devices (lines and trunks) to always use an MTP. If the configuration parameters are set to not use an MTP (default case), Cisco Unified Communications Manager will attempt to dynamically allocate an MTP if the DTMF methods for the call are not compatible.
For example, phones that are running SCCP support only out-of-band DTMF, and Cisco Unified IP Phones using SIP (7905, 7912, 7940, 7960) support only RFC2833. Because the DTMF methods are not identical, Cisco Unified Communications Manager will dynamically allocate an MTP. If, however, a phone that is running SCCP that supports RFC2833 and out of band, such as Cisco Unified IP Phone 7971, calls a Cisco Unified IP Phone 7940 that is using SIP, Cisco Unified Communications Manager will not allocate an MTP because both phones support RFC2833. By having the same type of DTMF method supported on each phone, no need for an MTP exists.

Although Cisco Unified Communications Manager provides an MTP Required check box for SIP IP phones, you should not check this check box for Cisco Unified IP Phones that are running SIP. (Only generic, third-party SIP IP phones use this check box.) Checking this check box can cause problems with Cisco Unified Communications Manager features such as shared lines. When this check box is not checked, Cisco Unified Communications Manager will still insert MTPs dynamically as needed. Thus, little or no benefit occurs in checking the MTP Required check box for Cisco Unified IP Phones.

Configure regions for SIP devices with the MTP required option enabled

When you configure a region relationship, you must ensure that you choose an audio codec that has sufficient bandwidth for all the devices that will be used in a call. This includes configuring the codec for devices that will be in the same region as well as devices that are in different regions. When you configure a trunk or third-party phone to use SIP and Media Termination Point Required is enabled, Cisco Unified Communications Manager Administration only allows you to choose a G.711 codec in the MTP Preferred Originating Codec field. When you assign the SIP trunk or third-party phone that is running SIP with the MTP Required option enabled to the device pool for that region, you must verify that the region relationship between the SIP device and the MTP device is configured to use a codec with equal or greater bandwidth (G.711 or Wideband/AAC-LD (mpeg4-generic) codec).

SIP service parameters

You can individually configure SIP timers and counters for functionality on different servers.

SIP Interoperability

The SIP Interoperability Enabled service parameter, which supports the Cisco CallManager service, determines whether Cisco Unified Communications Manager supports Session Initiation Protocol (SIP) for SIP stations and SIP trunks. Devices that run SIP, for example, phones and trunks, require that you set this parameter to True; when you set this parameter to False, Cisco Unified Communications Manager ignores SIP messages, and SIP devices do not function; that is, phones that run SIP cannot register with Cisco Unified Communications Manager and SIP trunks cannot interact with Cisco Unified Communications Manager. The default value specifies True. You must restart the Cisco CallManager service if you change the value of this parameter.

SIP timers and counters

SIP timers and counters act as configurable service parameters. The following tables describe the various SIP timers and counters and give their default values and range values:
### Table 31: SIP Timers That Are Supported in Cisco Unified Communications Manager

<table>
<thead>
<tr>
<th>Timer</th>
<th>Default Value</th>
<th>Default Range</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trying</td>
<td>500 milliseconds</td>
<td>100 to 1000</td>
<td>Time that Cisco Unified Communications Manager should wait for a 100 response before retransmitting the INVITE.</td>
</tr>
<tr>
<td>Connect</td>
<td>500 milliseconds</td>
<td>100 to 1000</td>
<td>Time that Cisco Unified Communications Manager should wait for an ACK response before retransmitting the 2xx response to the INVITE.</td>
</tr>
<tr>
<td>Disconnect</td>
<td>500 milliseconds</td>
<td>100 to 1000</td>
<td>Time that Cisco Unified Communications Manager should wait for a 2xx response before retransmitting the BYE request.</td>
</tr>
<tr>
<td>Expires</td>
<td>180000 milliseconds</td>
<td>60000 to 300000</td>
<td>Valid time that is allowed for an INVITE request.</td>
</tr>
<tr>
<td>rel1xx</td>
<td>500 milliseconds</td>
<td>100 to 1000</td>
<td>Time that Cisco Unified Communications Manager should wait before retransmitting the reliable1xx responses.</td>
</tr>
<tr>
<td>PRACK</td>
<td>500 milliseconds</td>
<td>100 to 1000</td>
<td>Time that Cisco Unified Communications Manager should wait before retransmitting the PRACK request.</td>
</tr>
<tr>
<td>PUBLISH</td>
<td>500 milliseconds</td>
<td>100 to 1000</td>
<td>This parameter specifies the maximum time, in milliseconds, that Cisco Unified Communications Manager will wait to re-send a PUBLISH request. If a response is not received before the time specified in this timer expires, Cisco Unified Communications Manager re-sends the request when this timer expires.</td>
</tr>
</tbody>
</table>

**Note**

When the SIP device is using TCP transport and a timer times out, the SIP device does not retransmit. The device relies on TCP to retry.

### Table 32: SIP Retry Counters That Are Supported in Cisco Unified Communications Manager

<table>
<thead>
<tr>
<th>Retry Counter</th>
<th>Default Value</th>
<th>Default Range</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>INVITE</td>
<td>6</td>
<td>1 to 10</td>
<td>Number of INVITE retries</td>
</tr>
<tr>
<td>Response</td>
<td>6</td>
<td>1 to 10</td>
<td>Number of RESPONSE retries</td>
</tr>
</tbody>
</table>
### Retry Counter

<table>
<thead>
<tr>
<th>Retry Counter</th>
<th>Default Value</th>
<th>Default Range</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>BYE</td>
<td>10</td>
<td>1 to 10</td>
<td>Number of BYE retries</td>
</tr>
<tr>
<td>Cancel</td>
<td>10</td>
<td>1 to 10</td>
<td>Number of Cancel retries</td>
</tr>
<tr>
<td>PRACK</td>
<td>6</td>
<td>1 to 10</td>
<td>Number of PRACK retries</td>
</tr>
<tr>
<td>Rel1xx</td>
<td>10</td>
<td>1 to 10</td>
<td>Number of Reliable 1xx response retries</td>
</tr>
<tr>
<td>PUBLISH</td>
<td>6</td>
<td>1 to 10</td>
<td>This parameter specifies the number of times that Cisco Unified Communications Manager re-sends the PUBLISH message.</td>
</tr>
</tbody>
</table>

### Supported audio media types

The following table describes the various supported audio media types:

#### Table 33: Supported Audio Media Types

<table>
<thead>
<tr>
<th>Type</th>
<th>Encoding Name</th>
<th>Payload Type</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>G.711 u-law</td>
<td>PCMU</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>GSM Full-rate</td>
<td>GSM</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>G.723.1</td>
<td>G723</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>G.711 A-law</td>
<td>PCMA</td>
<td>8</td>
<td></td>
</tr>
<tr>
<td>G.722</td>
<td>G722</td>
<td>9</td>
<td></td>
</tr>
<tr>
<td>G.722.1</td>
<td>G7221</td>
<td>Dynamically Assigned</td>
<td>Acceptable range comprises 96 - 127</td>
</tr>
<tr>
<td>G.728</td>
<td>G728</td>
<td>15</td>
<td></td>
</tr>
<tr>
<td>G.729</td>
<td>G729</td>
<td>18</td>
<td>Support all combinations of annex A and B</td>
</tr>
<tr>
<td>RFC2833 DTMF</td>
<td>Telephony-event</td>
<td>Dynamically Assigned</td>
<td>Acceptable range comprises 96 - 127</td>
</tr>
<tr>
<td>AAC-LD (mpeg4-generic)</td>
<td>mpeg4-generic</td>
<td>Dynamically Assigned</td>
<td>Acceptable range comprises 96 - 127</td>
</tr>
</tbody>
</table>
### Supported video media types

The following table describes the various supported video media types:

**Table 34: Supported Video Media Types**

<table>
<thead>
<tr>
<th>Type</th>
<th>Encoding Name</th>
<th>Payload Type</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAC-LD (MP4A-LATM)</td>
<td>MP4A-LATM</td>
<td>Dynamically Assigned</td>
<td>Acceptable range comprises 96 - 127</td>
</tr>
<tr>
<td>ILBC</td>
<td>iLBC</td>
<td>Dynamically Assigned</td>
<td>Acceptable range comprises 96 - 127</td>
</tr>
<tr>
<td>AMR</td>
<td>AMR</td>
<td>Dynamically Assigned</td>
<td>Acceptable range comprises 96 - 127</td>
</tr>
<tr>
<td>AMR-WB</td>
<td>AMR-WB</td>
<td>Dynamically Assigned</td>
<td>Acceptable range comprises 96 - 127</td>
</tr>
</tbody>
</table>

### Supported application media type

The following table describes the supported application media types:

**Table 35: Supported Application Media Types**

<table>
<thead>
<tr>
<th>Type</th>
<th>Encoding Name</th>
<th>Payload Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>H.261</td>
<td>H261</td>
<td>31</td>
</tr>
<tr>
<td>H.263</td>
<td>H263</td>
<td>34</td>
</tr>
<tr>
<td>H.263+</td>
<td>H263-1998</td>
<td>Acceptable range comprises 96 - 127</td>
</tr>
<tr>
<td>H.263++</td>
<td>H263-2000</td>
<td>Acceptable range comprises 96 - 127</td>
</tr>
<tr>
<td>H.264</td>
<td>H264</td>
<td>Acceptable range comprises 96 - 127</td>
</tr>
</tbody>
</table>

### Supported T38fax payload type

The following table describes the various supported application media types:
SIP profiles for trunks

SIP trunks and SIP endpoints use SIP profiles. SIP trunks use SIP profiles to define the Default Telephony Event Payload Type, the Disable Early media on 180, and the Reroute Incoming Request to new Trunk based on configuration. For more information on SIP profiles, see the SIP profiles for endpoints, on page 444.

SIP trunk security profiles

Cisco Unified Communications Manager Administration groups security-related settings for the SIP trunk to allow you to assign a single security profile to multiple SIP trunks. Security-related settings include device security mode, digest authentication, and incoming/outgoing transport type settings. You apply the configured settings to the SIP trunk when you choose the security profile in the Trunk Configuration window.

SIP UDP port throttling

SIP UDP port throttle thresholds help prevent Denial of Service (DOS) attacks from SIP trunks and SIP stations. When the incoming packet rate exceeds the configured threshold for a SIP station or SIP trunk UDP port, Cisco Unified Communications Manager throttles (drops) the packets that exceed the threshold. These throttle thresholds apply only to SIP UDP ports and do not affect SIP TCP or TLS ports.

Tip

Be aware that the enterprise parameter Denial-of-Service Protection Flag must be set to True for these parameter values to take effect.

The following table describes the configurable threshold values:

<table>
<thead>
<tr>
<th>Service Parameter</th>
<th>Default Value</th>
<th>Range</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP Station UDP Port Throttle Threshold</td>
<td>50</td>
<td>10-500</td>
<td>The SIP Station UDP Port Throttle Threshold parameter defines the maximum incoming packets per second that Cisco Unified Communications Manager can receive from a single (unique) IP address that is directed at the SIP station UDP port. When the threshold is exceeded, Cisco Unified Communications Manager throttles (drops) the packets that exceed the threshold.</td>
</tr>
</tbody>
</table>
The SIP Trunk UDP Port Throttle Threshold defines the maximum incoming packets per second that a SIP trunk can receive from a single (unique) IP address that is directed at the SIP trunk UDP port. When the threshold is exceeded, Cisco Unified Communications Manager throttles (drops) the packets that exceed the threshold.

If the incoming packet rate on a SIP trunk UDP port from a single IP address exceeds the configured SIP Trunk UDP Port Throttle Threshold during normal traffic, reconfigure the threshold. When a SIP trunk and SIP station share the same incoming UDP port, Cisco Unified Communications Manager throttles packets based on the higher of the two service parameter values. You must restart the Cisco CallManager service for changes to these parameters to take effect.

## SIP trunks between releases of Cisco Unified CallManager and Cisco Unified Communications Manager

Cisco Unified Communications Manager Release 6.0 (and later) and Cisco Unified CallManager Release 4.0 (and later, including 5.x) support TCP and UDP as Transport Types when they are used with SIP trunks. However, release 4.x uses one TCP connection per SIP call; releases 5.x and 6.x and later support multiple SIP calls over the same TCP connection (referred to as TCP connection reuse).

The following Cisco products support TCP; however, not all support TCP Reuse:

- Cisco Unified CallManager Release 4.1 - No TCP Connection Reuse
- Cisco Unified CallManager Release 4.2 - No TCP Connection Reuse
- Cisco Unified CallManager Release 5.0(2) - TCP Connection Reuse
- Cisco Unified CallManager Release 5.1(x)- TCP Connection Reuse
- Cisco Unified Communications Manager Release 6.0(x) and later - TCP Connection Reuse
- Cisco IOS 12.3(8)T and above - TCP Reuse
- Cisco IOS 12.3(8)T and below - No TCP Reuse

The following table lists the SIP trunk connectivity that is supported among Cisco Unified CallManager and Cisco Unified Communications Manager releases and the IOS gateway.
Table 38: SIP Trunk Compatibility Matrix

<table>
<thead>
<tr>
<th></th>
<th>Cisco Unified CallManager Release 4.x</th>
<th>Cisco Unified CallManager 5.x and Cisco Unified Communications Manager 6.x</th>
<th>IOS 12.3(8)T</th>
<th>Below IOS 12.3(8)T</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Unified CallManager Release 4.x</td>
<td>UDP/TCP</td>
<td>UDP only</td>
<td>UDP only</td>
<td>UDP/TCP</td>
</tr>
<tr>
<td>Cisco Unified CallManager 5.x and Cisco Unified Communications Manager 6.x and later</td>
<td>UDP only</td>
<td>UDP/TCP</td>
<td>UDP/TCP</td>
<td>UDP only</td>
</tr>
<tr>
<td>IOS 12.3(8)T</td>
<td>UDP only</td>
<td>UDP/TCP</td>
<td>UDP/TCP</td>
<td>UDP only</td>
</tr>
<tr>
<td>Below IOS 12.3(8)T</td>
<td>UDP/TCP</td>
<td>UDP only</td>
<td>UDP only</td>
<td>UDP/TCP</td>
</tr>
</tbody>
</table>

If a Release 6.x (or later) system makes multiple calls over a TCP-based SIP trunk to a 4.x system, the 4.x system will only connect one call. The rest of the calls will not get connected. When using SIP trunks between 4.x and 6.x (or later) systems, you must configure both systems to use UDP as the Outgoing Transport Type, so calls between the release 4.x and 6.x (or later) systems will connect properly.

To configure UDP, use Cisco Unified Communications Manager Administration:

- For Cisco Unified Communications Manager Release 6.0 (and later) that is connecting to a Release 4.x system, choose UDP as the Outgoing Transport Type from the SIP Trunk Security Profile Configuration window.
- For Cisco Unified CallManager Release 4.0 (and later) that is connecting to a Release 6.x (or later) system, choose UDP as the Outgoing Transport Type from the Trunk Configuration window.

**SIP forking for SIP trunk**

Call setup (INVITE) requests sent by Cisco Unified Communications Manager on a SIP trunk may be replicated and forwarded to multiple destinations by a SIP proxy (called forking). Cisco Unified Communications Manager supports forking, subject to the following limitations:

- Cisco Unified CallManager Release 4.x does not accept provisional responses (such as 180 Ringing) from more than five destinations. It does not accept a successful response (200 Ok) from any destination that is not among the first five to respond.

- Cisco Unified CallManager Release 5.x and Cisco Unified Communications Manager Release 6.x do not accept provisional responses (such as 180 Ringing) from more than 20 destinations. They do not accept a successful response (200 Ok) from any destination that is not among the first 20 to respond.
• If Cisco Unified CallManager Releases 4.x, Cisco Unified CallManager Release 5.x, and Cisco Unified Communications Manager Release 6.x accept a provisional response (183 Session Progress) that contains a session (media) description, they do accept a successful (200 Ok) response only from the same destination, and they will not accept any change in the session description from the provisional response to the successful response.

• If Cisco Unified CallManager Releases 4.x, Cisco Unified CallManager Release 5.x, and Cisco Unified Communications Manager Release 6.x are configured to acknowledge provisional responses (with the SIP PRACK method), Cisco Unified Communications Manager will not accept provisional responses and/or a successful response from any destination other than the first one to respond.

No other configuration options affect Cisco Unified Communications Manager support of downstream SIP forking.

**SIP transparency and normalization**

Cisco Unified Communications Manager can connect to a variety of endpoints, including PBXs, gateways, and service providers. Each endpoint may implement the SIP protocol differently, which can cause a unique set of interoperability issues. SIP transparency and normalization allow Cisco Unified Communications Manager to interoperate seamlessly with a variety of PBXs and service providers. Normalization allows you to modify incoming and outgoing SIP messages at a protocol level on their way through Cisco Unified Communications Manager. Transparency allows Cisco Unified Communications Manager to pass headers, parameters, and content bodies from one call leg to another.

**Normalization**

To normalize messages, Cisco Unified Communications Manager allows you to add or update scripts to the system and then associate the scripts with one or more SIP trunks or SIP lines. The normalization scripts that you create allow you to preserve, remove, or change the contents of any SIP headers or content bodies, known or unknown. Normalization scripts can be applied to either SIP trunks in the Trunk Configuration window or they can be applied to SIP lines in the SIP Profile Configuration window.

For inbound messages, normalization occurs just after receiving the message from the network. For outbound messages, normalization occurs just prior to sending the message to the network. Normalization applies to any SIP trunk or SIP line with a script configured against the trunk or SIP profile in Cisco Unified Communications Manager, regardless of the type of device to which the trunk connects on the other side. Normalization occurs per call leg and does not require the other call leg to be SIP. The call can specify SIP line to SIP trunk, SCCP to SIP trunk, MGCP to SIP trunk, H.323 to SIP trunk, and so on.

The script environment (and thus context) is maintained over the life of the SIP trunk or SIP device until the trunk gets reset or the device is reset. The script writer implements a Lua module and provides a set of callback functions to manipulate messages (for example, inbound_INVITE, outbound_180_INVITE, and so on). The environment makes the SIP message and SDP (if present) accessible via a set of APIs.

The Cisco script environment controls memory consumption. If a script exceeds its configured memory usage threshold, an error occurs.

**Transparency**

Transparency refers to the ability to pass information from one call leg to the other. SIP transparency allows inbound SIP message information, such as proprietary headers, to pass through from one side of the Cisco Unified Communications Manager to the other so that the information gets included in the outbound SIP message.
Transparent pass-through only applies to a SIP trunk to SIP trunk call.

In this release, Cisco Unified Communications Manager supports transparency for the following message types:

- Unknown header (pass-through)
- Unknown parameter (pass-through)
- Unknown content body (pass-through)
- Initial INVITE, reINVITE, UPDATE, INFO, BYE, 18x, 200 (INVITE, UPDATE), 4/5/6xx
- One-to-one transaction when possible (in other words, reINVITE triggers one reINVITE on the other side)

For more information on transparency, see the Developer Guide for SIP Transparency and Normalization.

You can also configure REFER transparency so that Cisco Unified Communications Manager passes on REFER requests to another endpoint rather than acting on them. REFER transparency is key in call center applications, where the agent sending the REFER (initiating the blind transfer) resides in a geographic area remote from both of the other call parties. With REFER transparency, the local Cisco Unified Communications Manager drops from the call when the local agent gets removed. Without REFER transparency, the call signaling remains connected through the Cisco Unified Communications Manager of the agent that initiates the transfer. The load associated with the call and continued use of MTP devices (if allocated during the initial call), remained with the Cisco Unified Communications Manager of the agent initiating the transfer, resulting in signaling delays between the parties in the new call.

You enable REFER transparency by associating the refer-passthrough script or a custom REFER transparency script with one or more SIP trunks on the Trunk Configuration window (Device > Trunk). You must configure the fields in the Normalization Script group box.

For information on creating customer scripts, refer to the Developer Guide for SIP Transparency and Normalization. To upload custom scripts in Cisco Unified Communications Manager, use the SIP Normalization Script Configuration window (Device > Device Settings > SIP Normalization Script).

**Tracing for SIP normalization**

Cisco Unified Communications Manager provides tracing for SIP normalization to provide the following functionality:

- To trace both the nonnormalized and the normalized message for the purpose of debugging call failures
- To allow scripts to produce traces for the purpose of debugging scripts
- To produce traces when scripts fail unexpectedly for the purpose of maintaining the system

To debug scripts and call failures, enable tracing by checking the SDI Enable SIP Call Processing check box on the Trace Configuration window in Cisco Unified Serviceability. This option allows you to trace incoming and outgoing SIP messages before and after normalization.

---

**Note**

SIP Normalization produces traces only if you enable tracing on the Normalization script.

To generate traces from the script for debugging purposes, check the Enable Trace check box that appears in Cisco Unified Communications Manager Administration in the Trunk Configuration window for SIP trunks.
or the SIP Profile Configuration window for SIP lines. When checked, the trace.output and trace.format APIs that are provided to the Lua script writer produce SDI trace.

---

**Note**

Cisco recommends that you enable tracing only while debugging a script. Tracing impacts performance and should not be enabled under normal operating conditions.

If you enable SDI tracing, Cisco Unified Communications Manager produces additional SDI error-level traces, including the following traces:

- Script failed to load
- Script execution error (bad argument)
- Script aborted (ran too long)

These traces include the following information:

- SIP trunk name or SIP profile name
- Lua script name
- Lua script line number where the failure occurred, if applicable
- Information specific to the failure

### Alarms for SIP normalization

Cisco Unified Communications Manager identifies SIP normalization script usage and errors; that is, the system keeps timestamps as to when the script opens and closes as well as when errors and resource warnings occur.

The system generates the following alarms:

- SIPNormalizationScriptOpened
- SIPNormalizationScriptClosed
- SIPNormalizationResourceWarning
- SIPNormalizationScriptError
- SIPNormalizationAutoResetDisabled

To find these alarms, access the CallManager Alarm Catalog in Cisco Unified Serviceability.

### Performance counters for SIP normalization

The Cisco SIP Normalization performance object contains counters that allow you to monitor aspects of the normalization script, including script status and errors. Performance counters operate slightly differently for SIP lines and SIP trunks:

- For SIP lines, each script has only one set of performance counters. This is true even if two endpoints share the same script.
• For SIP trunks, each device that has an associated script causes a new instance of these counters to be created. When you disassociate a script from the device, or remove the device from Cisco Unified Communications Manager Administration, the instance of these counters gets removed.

For more information on performance counters, see the Cisco Unified Real-Time Monitoring Tool Administration Guide.

Dependency records

To find trunks that use a specific normalization script, choose Dependency Records from the Related Links drop-down list box that is provided on the Cisco Unified Communications Manager Administration SIP Normalization Script Configuration window. The Dependency Records Summary window displays information about trunks that are using the script. To find more information about a specific trunk, click the Trunk link; then, click the name of the trunk from the Dependency Records Details window. If dependency records are not enabled for the system, the dependency records summary window displays a message.

SIP functions that are supported in Cisco Unified Communications Manager

Cisco Unified Communications Manager supports the functions and features in this section for SIP calls.

Basic calls between SIP endpoints and Cisco Unified Communications Manager

This section includes three basic calling scenarios. Two scenarios describe incoming and outgoing calls, while the other one describes the use of early media, which is a media connection prior to the connection or answer of a call.

Basic outgoing call

You can initiate outgoing calls to a SIP device from any Cisco Unified Communications Manager device. A Cisco Unified Communications Manager device includes SCCP or SIP IP phones or fax devices that are connected to Foreign Exchange Station (FXS) gateways. For example, an SCCP IP phone can place a call to a SIP endpoint. The SIP device that answers the call triggers media establishment.

Basic incoming call

Any device on the SIP network, including SIP IP phones or fax devices that are connected to FXS gateways, can initiate incoming calls. For example, a SIP endpoint can initiate a call to an SCCP IP phone. The SCCP IP phone that answers the call triggers media establishment.

Use of early media

While the PSTN provides inband progress information to signal early media (such as a ring tone or a busy signal), the same thing does not occur for SIP. The originating party includes Session Description Protocol (SDP) information, such as codec usage, IP address, and port number, in the outgoing INVITE message. In response, the terminating party sends its codec, IP address, and port number in a 183 Session Progress message to indicate possible early media.
The 183 Session Progress response indicates that the message body contains information about the media session. Both 180 Alerting and 183 Session Progress messages may contain SDP, which allows an early media session to be established prior to the call being answered.

When early media needs to be delivered to SIP endpoints prior to connection, Cisco Unified Communications Manager always sends a 183 Session Progress message with SDP. Although Cisco Unified Communications Manager does not generate a 180 Alerting message with SDP, it does support the 180 Alerting message with SDP when it receives one.

The SIP Profile Configuration window contains a Disable Early Media on 180 check box. Check the check box to play local ringback on the called phone and connect the media upon receipt of the 200OK response.

### DTMF relay calls between SIP endpoints and Cisco Unified Communications Manager

MTPs now dynamically get allocated, if needed, based on the DTMF methods that are used on each endpoint.

#### Forward DTMF digits from SIP devices to gateways or Interactive Voice Response (IVR) systems for dissimilar DTMF methods

The following figure shows the MTP software device that is processing inband DTMF digits from the phone that is running SIP to communicate with the Primary Rate Interface (PRI) gateway. The RTP stream carries RFC 2833 DTMF, as indicated by a dynamic payload type.

![Figure 40: Forwarding DTMF Digits](image)

The previous figure begins with media streaming, and the MTP device has been informed of the DTMF dynamic payload type.

1. The phone that is running SIP initiates a payload type response when the user enters a number on the keypad. The phone that is running SIP transfers the DTMF inband digit (per RFC 2833) to the MTP device.
2. The MTP device extracts the inband DTMF digit and passes the digit out of band to Cisco Unified Communications Manager.
3. Cisco Unified Communications Manager then relays the DTMF digit out of band to the gateway or IVR system.

#### Generate DTMF digits for dissimilar DTMF methods

As discussed in DTMF relay calls between SIP endpoints and Cisco Unified Communications Manager, on page 411, SIP sends DTMF inband digits, while Cisco Unified Communications Manager only supports
out-of-band digits. The software MTP device receives the DTMF out-of-band tones and generates DTMF inband tones to the SIP client.

**Figure 41: Generating DTMF Digits**

![Diagram showing the process of generating DTMF digits]

The figure shown begins with media streaming, and the MTP device has been informed of the dynamic DTMF payload type.

1. The SCCP IP phone user presses buttons on the keypad. Cisco Unified Communications Manager collects the out-of-band digits from the SCCP IP phone.

2. Cisco Unified Communications Manager passes the out-of-band digits to the MTP device.

3. The MTP device converts the digits to RFC 2833 RTP-compliant inband digits and forwards them to the SIP client.

**Supplementary services that are initiated if an MTP is allocated**

The system supports all supplementary services that the SCCP endpoint initiates during a SIP call. Cisco Unified Communications Manager internally manages SCCP endpoints without affecting the connecting SIP device. Any changes to the original connecting information get updated with re-INVITE or UPDATE messages that use the Remote-Party-ID header. See SIP Extensions for Caller Identity and Privacy for more information on the Remote-Party-ID header.

The Ringback tone during blind transfer, on page 412 describes a blind transfer, which is unique as a supplementary service because it requires Cisco Unified Communications Manager to provide a media announcement.

**Ringback tone during blind transfer**

For SCCP-initiated blind transfers, Cisco Unified Communications Manager needs to generate tones or ringback after a call already has connected. In other words, Cisco Unified Communications Manager provides a media announcement for blind transfers.

A blind transfer works when the transferring phone connects the caller to a destination line before the target of the transfer answers the call. A blind transfer differs from a consultative, or attended transfer, in which one transferring party either connects the caller to a ringing phone (ringback received) or speaks with the third party before connecting the caller to the third party.
Blind transfers that are initiated from an SCCP IP phone allow ringback to the original, connected SIP device user. To accomplish ringback, Cisco Unified Communications Manager uses an annunciator software device that is often located with an MTP device.

With an annunciator, Cisco Unified Communications Manager can play predefined tones and announcements to SCCP IP phones, gateways, and other IP telephony devices. These predefined tones and announcements provide users with specific information on the status of the call.

**Supplementary services that are initiated by SIP endpoint**

The sections which follow describe supplementary services that a SIP endpoint can initiate.

**SIP-initiated call transfer**

Cisco Unified Communications Manager supports SIP-initiated call transfer and accepts REFER requests or INVITE messages that include a Replaces header.

**Call hold**

Cisco Unified Communications Manager supports call hold and retrieve that a SIP device initiates or that a Cisco Unified Communications Manager device initiates. For example, when a SCCP IP phone user retrieves a call that another user placed on hold, Cisco Unified Communications Manager sends a re-INVITE message to the SIP proxy. The re-INVITE message contains updated Remote-Party-ID information to reflect the current connected party. If Cisco Unified Communications Manager originally initiated the call, the Party field in the Remote-Party-ID header gets set to calling; otherwise, it gets set to called. For more information on the Party field parameter, see Enhanced Call Identification services, on page 413.

**Call forward**

Cisco Unified Communications Manager supports call forward that a SIP device initiates or that a Cisco Unified Communications Manager device initiates. With call forwarding redirection requests from SIP devices, Cisco Unified Communications Manager processes the requests. For call forwarding that is initiated by Cisco Unified Communications Manager, the system uses no SIP redirection messages. Cisco Unified Communications Manager handles redirection internally and then conveys the connected party information to the originating SIP endpoint through the Remote-Party-ID header.

**Enhanced Call Identification services**

This section describes the following SIP identification services in Cisco Unified Communications Manager and how Cisco Unified Communications Manager conveys these identification services in the SIP:

- **Line Identification Services**
  - Calling Line Presentation (CLIP) and Restriction (CLIR)
  - Connected Line Presentation (COLP) and Restriction (COLR)

- **Name Identification Services**
  - Calling Name Presentation (CNIP) and Restriction (CNIR)
Cisco Unified Communications Manager provides flexible configuration options to provide these identification services either on a call-by-call or a statically preconfigured for each SIP signaling interface basis.

**Related Topics**

 Caller Identification support with device control protocols in Cisco Unified Communications Manager, on page 188

### Call line and name identification presentation

Cisco Unified Communications Manager includes the calling line (or number) and name presentation information in the From and Remote-Party-ID headers of the initial INVITE message from Cisco Unified Communications Manager. The From header field indicates the initiator of the request. Cisco Unified Communications Manager uses Remote-Party-ID headers in 18x, 200 and re-INVITE messages to convey connected name and identification information. The Remote-Party-ID header also gives detailed descriptions of caller identity and privacy. Cisco Unified Communications Manager sets the Party field of the Remote-Party-ID header to calling for calling ID services.

**Note**

See the Cisco IOS SIP Configuration Guide for more general information on Remote-Party-ID header.

**Example:**

Bob Jones (with external phone number=8005550100) dials out to a SIP signaling interface; the From and Remote-Party-ID headers contain

```
From: “Bob Jones” <sip:8005550100@localhost>
Remote-Party-ID: “Bob Jones”<8005550100@localhost; user=phone>; party=calling;screen=no;privacy=off
```

### Call line and name identification restriction

Calling line (or number) and name restrictions configuration occurs on the SIP signaling interface level or on a call-by-call basis. The SIP trunk level configuration takes precedence over the call-by-call configuration. To configure on a call-by-call basis, see Enhanced Call Identification services, on page 413 in the Cisco Unified Communications Manager Administration Guide.

Calling line and name restrictions configuration also occurs independently of each other. For example, you may choose to restrict only numbers and allow names to be presented.

**Example 1**

With a restricted calling name, Cisco Unified Communications Manager sets the calling name in the From header to a configurable string. Cisco Unified Communications Manager sets the display field in the Remote-Party-ID header to include the actual name but sets the Privacy field to name:

```
From: “Anonymous” <sip:8005550100@localhost>
Remote-Party-ID: “Bob Jones”<sip:9728135001@localhost; ;user=phone>; party=calling;screen=no;privacy=name
```
Example 2

With a restricted calling number, Cisco Unified Communications Manager leaves out the calling line in the From header; however, Cisco Unified Communications Manager still includes the calling line in the Remote-Party-ID header but sets the Privacy field to privacy=uri:

From: “Bob Jones” <sip:@localhost>
Remote-Party-ID: “Bob Jones”<sip:8005550100@localhost; ;user=phone>;
party=calling;screen=no;privacy=uri

Example 3

With a restricted calling name and number, Cisco Unified Communications Manager sets the Privacy field to privacy=full in the Remote-Party-ID header:

From: “Anonymous” <sip:localhost>
Remote-Party-ID: “Bob Jones”<sip:8005550100@localhost;user=phone>;
party=calling;screen=no;privacy=full

SIP CLI Handling Change

Cisco Unified Communications Manager 9.0 provides a SIP feature that delivers two sets of calling party identities for outgoing SIP calls, and allows selective CLI (Calling Line Identification) for incoming SIP calls based on SIP headers.

Outgoing SIP Call with two sets of Identities

When switch-board data is configured on a SIP Trunk, the original caller identification is not overwritten by the data in the SIP headers, for the outgoing sip messages, when the Maintain Original Caller ID DN and Caller Name in Identity Headers are checked.

Outgoing SIP Call with two set of Identities - SIP Line

When Maintain Original Caller ID DN and Caller Name in Identity Headers are configured on the SIP Trunk, all outgoing SIP calls are impacted. This feature can also be configured for groups of SIP line devices via SIP Profiles. On the phone section of the SIP profile page, two new text boxes were added named Caller ID DN and Caller Name to mirror the switch-board data on a SIP Trunk. On the trunk section of SIP profile a new checkbox was added called Allow Passthrough of Configured Line Device Caller Information.

Incoming CLI for SIP Calls

Cisco Unified Communications Manager allows you to enhance identity selection, presentation and restriction on SIP interfaces. The addition of new configuration fields used for presentation on the SIP Trunk as well as on the SIP profiles to control corresponding SIP phones provides this new functionality.

With the introduction of the Outgoing Identity feature, an incoming SIP call can have two sets of calling party identities. Incoming CLI (Calling Line Identification) was introduced to aid in selecting the identity for call processing. Selection is controlled via a new list box for Calling Line Identification Presentation.

In some networks, there are two sets of identities maintained, network provided identity (trusted) and user provided identity (non-trusted). In terms of SIP calls, identity headers including P-Asserted-Identity (PAI), P-Preferred-Identity (PPI) and Remote-Party-ID (RPID) carry the network provided identity, while the FROM header carries the user provided identity. Previous releases of Cisco Unified Communications Manager provided only a single set of identities for outgoing calls. The identities in the identity headers and FROM headers were exactly the same and there was no way to differentiate between the network provided identity
and the user provided identity. Typically, the administrator configures each user device with a Directory Number (DN) and a display name. An outgoing call from this DN would carry its directory number and display name in both Identity headers and the FROM header. Administrators can also configure another identity on a SIP trunk. This identity, sometimes called a switchboard identity, is used to hide each individual caller's identity. It can be configured on the Caller Information section of a SIP Trunk for outbound calls. The configuration includes two fields, **Caller ID DN** and **Caller Name**. The caller's original directory number and display name are overwritten when such configurations are enabled.

Cisco Unified Communications Manager 9.0 provides configurations where the administrator can enable both the switchboard identity and original caller identity. The switchboard identity is carried in the FROM header and original caller identity will be carried in Identity headers. Such configuration can be enabled for each SIP Trunk or SIP user device.

For the incoming calls from within the network, Cisco Unified Communications Manager provides configurations to accept the network provided identity carried in Identity headers or the user provided identity carried in FROM header. Cisco Unified Communications Manager maintains a single set of identities per call.

---

**Note**

As of Cisco Unified Communications Manager 7.0.1, three different identity headers are supported, PAI, PPI and RPID. Depending on the Call Routing Information configuration on the SIP trunk page, one or two of these headers may be present in an outgoing request or response.

Outgoing Call with Original Caller Identity is configured by default in the Call Routing Information. By default the **Remote-Party-Id** and **Asserted-Identity** checkboxes are checked and the **Asserted-Type** and **SIP Privacy** fields are set to Default.

To configure an outgoing call with the switchboard identity, set the Caller ID DN and Caller Name on the Calls section of SIP Trunk configuration page. These provide the switchboard identity and hide the caller's identity.

For calls originated from Cisco Unified Communications Manager devices, the Identity headers are set to the line ID of the device and the From header is set to either the same as the Identity header or the switchboard information. This is provision-able and does not require changes in Cisco Unified Communications Manager. On the SIP Trunk Configuration page, there is a new checkbox for **Maintain Original Caller ID DN** and **Caller Name in Identity Headers** which is used to control the display name and number of outgoing SIP messages. When enabled for the outgoing SIP messages, the configured value Caller ID DN will not override the phone number and the configured Caller Name will not overwrite the caller name in outgoing Identity headers.

---

**Connected line and name identification presentation**

Cisco Unified Communications Manager uses connected line and name identification as a supplementary service to provide the calling party with the connected party number and name. The From header field indicates the initiator of the request. Cisco Unified Communications Manager uses Remote-Party-ID headers in 18x, 200, and re-INVITE messages to convey connected information. Cisco Unified Communications Manager sets the Party field of Remote-Party-ID header to called.

**Example 1**

Cisco Unified Communications Manager receives an INVITE message with a destination address of 800555. Cisco Unified Communications Manager includes the connected party name in 18x and 200 messages as follows:
Connected line and name identification restriction

You can configure connected line (or number) and name restrictions on the SIP trunk level or on a call-by-call basis. The SIP trunk level configuration takes precedence over the call-by-call configuration.

Similar to Calling ID services, users can restrict connected number and name independently of each other.

Example 1

Cisco Unified Communications Manager sets the display field in the Remote-Party-ID header to include the actual name but sets the Privacy field to privacy=name:

Remote-Party-ID: “Bob Jones”<8005550100@localhost; user=phone>; party=called;screen=no;privacy=name

Example 2

With a restricted connected number, Cisco Unified Communications Manager still includes the connected number in the Remote-Party-ID header but sets the Privacy field to privacy=uri:

Remote-Party-ID: “Bob Jones”<8005550100@localhost; user=phone>; party=called;screen=no;privacy=uri

Example 3

With a restricted connected name and number, Cisco Unified Communications Manager sets the Privacy field to privacy=full in the Remote-Party-ID header:

Remote-Party-ID: “Bob Jones”<8005550100@localhost; user=phone>; party=called;screen=no;privacy=full

Redirecting Dial Number Identification Service (RDNIS)

Cisco Unified Communications Manager uses the SIP Diversion header in the initial INVITE message to carry available RDNIS information.

Note

When a call gets redirected from a DN to a voice-mail server/service that is integrated with Cisco Unified Communications Manager using a SIP trunk, the voice mailbox mask on the voice-mail profile for the phone modifies the diverting number in the SIP Diversion header. This behavior is expected because the diversion header gets used by the Cisco Unified Communications Manager server to choose a mailbox.

Redirection

The following scenario represents the behavior that you will get if the Redirect by Application check box on the SIP Profile Configuration window is unchecked. Previously, the redirection from the SIP network got handled at the SIP stack level, and the system accepted and forwarded all redirection requests to the contacts in the redirection response out to the same trunk on which the redirection response was received. No consulting
or applying of any additional logic to handle or restrict how the call is redirected occurred. For example, if the redirection contact in a 3xx response to an outgoing INVITE was a Cisco Unified Communications Manager registered phone and the stack is handling redirection, the call gets redirected back out over the same trunk instead of being routed directly to the Cisco Unified Communications Manager phone. Getting redirected to a restricted phone number (such as an international number) means that handling redirection at the stack level will cause the call to be routed instead of being blocked.

Checking the Redirect by Application check box that is on the SIP Profile Configuration window and configuring this option on the SIP trunk allows the Cisco Unified Communications Manager administrator to

- Apply a specific calling search space to redirected contacts that are received in the 3xx response.
- Apply digit analysis to the redirected contacts to make sure that the call gets routed correctly.
- Prevent DOS attack by limiting the number of redirection (recursive redirection) that a service parameter can set.
- Allow other features to be invoked while the redirection is taking place.

For more information, see the Enhanced Call Identification services, on page 413.

**Support of G. Clear codec for SIP trunks**

The G. Clear (Clear channel) codec enables tandem switching of Digital Signal-0 (DS-0) data circuits through a voice network that uses SIP trunks and Cisco Unified Communications Manager. The G.Clear codec uses 64 kb/s of bandwidth (not including IP packet overhead), which is similar to the G.711 codec. The Cisco Unified Communications Manager selects the codec of a voice call and prioritizes the G. Clear codec ahead of the G.711 mulaw and G.711 alaw codecs in the media table.

You may require the G.Clear codec or the G.729 codec in a region or some other low-bandwidth codec for calls to remote regions. The G.729 codec, which is optimized for speech, uses significantly less bandwidth than the G. Clear codec. Be aware that the G.Clear codec is an option only to explicitly allow it to run in lower bandwidth regions.

G. Clear codec calls require separate Differentiated Services Code Point (DSCP) values in the header of IP packets. This differs from traditional voice codecs and video calls and must be tagged uniquely by the MLPP precedence level. Service parameters apply these capabilities.

G. Clear codec calls maintain consistency throughout the gateway by using the RTP dynamic payload type 125. The dynamic payload type gets statically allocated by using Cisco Unified Communications Manager. SIP trunk support for the G. Clear codec provides intercluster operability. The codec, which is negotiated as a supported media type in SIP Session Description Protocol (SDP) messaging, gets statically encoded to RTP payload type 125.

---

**Note**

No G. Clear codec support exists for media termination points.

Support exists for ISDN bearer capability for incoming ISDN data calls (restricted and unrestricted digital) that exit the VoIP network on another T1 PRI trunk.
The following figure shows a typical SIP trunk deployment that has the G.Clear codec enabled.

**Figure 42: SIP Trunk Deployment with G. Clear Codec**

Two SIP service parameters enable the G. Clear codec over SIP trunks: SIP Route Class Naming Authority and SIP Clear Channel Data Route Class Label. The SIP Route Class Naming Authority parameter represents the naming authority and context for the labels that are used in SIP signaling that represent the route class. The value specifies a domain name that is owned by the naming authority. The default specifies cisco.com.

To signal a particular route class value, Cisco Unified Communications Manager incorporates the domain name and the appropriate route class label, as defined in the SIP Clear Channel Data Route Class Label service parameter, into the SIP signaling.

The SIP Clear Channel Data Route Class Label represents the clear channel data route class in SIP signaling. This parameter and the SIP Route Class Naming Authority parameter create the complete signaling syntax for the SIP clear channel data route class value. The default specifies cedata.

Route class signaling proves useful when you are interworking with TDM networks that make routing decisions based on route class and clear-channel data route classes. The default domain name that is specified in the parameter applies to interaction between Cisco switches. You can change the parameter to any vendor– or deployment–specific requirements. The far-end switch should receive the same value that is configured in the parameter.

The following entities do not get supported or are disabled:

- H.323 ICTs with the G. Clear codec do not get supported.
- Skinny Client Control Protocol (SCCP) devices with the G. Clear codec do not get supported.
- T1 and E1 CAS with the G. Clear codec do not get supported.
- RSVP with the G. Clear codec does not get supported.
- MLPP over E1 trunks does not get supported.
- Echo cancellation and zero suppression for outbound G. Clear codec calls get disabled.
- Frame aligning individual DS-0 circuits that transit the VoIP network do not get supported because terminal equipment takes responsibility for the bonding of the individual DS-0 circuits that are defined by ITU H.244.
- Fast Start and Media Termination Point Required options in Cisco Unified Communications Manager do not work with G. Clear that is enabled.
- DTMF signaling with the G.Clear codec does not get supported
Cisco Unified Communications Manager ignores DTMF configuration settings for all calls on which G.Clear is advertised in the list of codecs, irrespective of whether G.Clear is chosen as the codec for the call.

**Early offer for G.Clear calls**

Cisco Unified Communications Manager supports limited early offer for G.Clear data calls (also known as clear channel). The Early Offer for G.Clear Calls feature provides support for third-party SIP user agents that can do early offer to negotiate data calls without using a Media Termination Point. MTPs do not support the G.Clear codec.

If you enable both Media Termination Point Required and Early Offer for G.Clear Calls for a SIP device, the system does not allocate the MTP if the G.Clear codec is present in the offer. The system only allocates the MTP if the call is not G.Clear, and the MTP is required.

The Early Offer for G.Clear Calls feature supports both standards-based G.Clear (CLEARMODE) and proprietary Cisco Session Description Protocols (SDP), including CCD, G.nX64, and X-CCD.

To enable or disable Early Offer for G.Clear Calls, choose one of the following options on the SIP Profile Configuration window in Cisco Unified Communications Manager Administration:

- Disabled (default)
- CLEARMODE
- CCD
- G.nX64
- X-CCD

**Support of Multilevel Precedence and Preemption for SIP trunks**

Cisco Unified Communications Manager Administration supports Voice over Secured IP (VoSIP) networks with Multilevel Precedence and Preemption (MLPP) for SIP trunks. It adds a Resource Priority and SIP-Reason header to messages. SIP-signaled resources are prioritized by Cisco Unified Communications Manager to free up those resources so that the networks can function during emergencies and congestion. Resource Priority Namespace Network Domains and Resource Priority Namespace Lists can be configured to enable prioritization as required.

**Resource Priority Namespace Network Domains**

The Resource Priority Namespace Network Domain in SIP signaling is similar to the ISDN precedence Information Element (IE) and ISDN User Part (ISUP) precedence parameters used in legacy TDM MLPP networks.

The Resource Priority Namespace Network Domain is included on outbound calls and based on translation patterns or route patterns directing the call to the SIP trunk. The following messages include the configured Resource Priority Namespace Network Domain:

- INVITE
• UPDATE
• REFER

For inbound calls, the network domain is compared to a list of acceptable network domains. The network domain of an incoming call is examined only if the call terminates to a Cisco Unified Communications Manager endpoint. For all other call types, the network domain is not validated against a local configuration. The configuration of acceptable network domains must be added to the SIP Profile.

SIP trunks can respond to updated precedence signals and the following supplementary services:

• Precedence Call Waiting
• Call Transfer
• Call Forwarding
• Three-way Calling

The following headers, mapping, and queuing are not supported:

• Accept-Resource-Priority header.
• Inclusion of RP header in PRACK and ACK.
• Mapping of precedence levels between namespaces.
• Call queuing and other non-MLPP services.

Support for secure V.150.1 Modem over IP over SIP trunks

Support for secure V.150.1 based Modem over IP (MoIP) communications between an IP STE and legacy (BRI or analog) Secure Terminal Equipment (STE) across a SIP trunk and an intercluster SIP trunk. SIP trunks transport the Session Description Protocol (SDP) information for outbound calls and signal Cisco Unified Communications Manager when MoIP SDP information is received for inbound calls. Devices can call between clusters by using SIP to negotiate a V.150.1 secure call.

Note

No configuration of MoIP over SIP trunks is required.

Support for G.729a and G.729b codecs over SIP trunks

G.729a and G.729b are low-bandwidth codecs that can be used for calls that are initiated over SIP trunks. Be aware that this feature is required for endpoints that do not support delayed media calls and do not want to use a higher-bandwidth codec, such as G.711.

Because an MTP needs to be pre-allocated for early-offer calls, you must configure an external MTP or transcoder device to use this feature. The software MTP does not support G.729 over SIP trunks.

Although this feature supports all four G.729 codecs (G.729, G.729a, G.729b, and G.729ab), the system cannot distinguish between G.729 and G.729a or between G.729b and G.729ab. Therefore, Cisco Unified Communications Manager Administration provides only two options for configuring these codecs on SIP trunks: G729/G729a and G729b/G729ab.
The G.729 codec over SIP trunks applies only to outgoing calls, and incoming calls are not affected. Be aware that the system does not support midcall codec switching from G.729 to any other codec.

Support for SIP T.38 interoperability with Microsoft Exchange

The T.38 standard comes from the ITU-T Recommendation for real-time transfer of Group 3 facsimile (fax) communication over IP networks. In Cisco Unified Communications Manager, the implementation of T.38 interoperability with Microsoft Exchange enables the system to switch a call from audio to T.38 fax.

The following steps show how the Microsoft Exchange Server establishes a call to a fax machine:

1. The exchange server establishes an audio call with the fax machine.
2. The fax machine send fax tones (CNG) to the exchange server.
3. The exchange server recognizes the fax tones and tries to renegotiate the call as a T.38 fax (or T.38 fax relay) call.

Cisco Unified Communications Manager Administration allows you to configure a SIP Profile that supports T.38 fax communication. This profile applies to SIP trunks only, not phones that are running SIP or endpoints.

Support for QSIG tunneling over SIP

Cisco Unified Communications Manager supports interworking between QSIG and SIP messages over a SIP trunk on the IP network toward another Cisco Unified Communications Manager or QSIG-SIP gateway to support QSIG calls and features, such as Message Waiting Indication (MWI), Call Transfer, Call Diversion, Call Back, Call Completion, Path Replacement, and Identification Services. To receive these features, Cisco Unified Communications Manager allows you to configure a SIP trunk with QSIG as the tunneled protocol. For information about how to configure SIP trunks, see Support of G.729 codec for SIP trunks, on page 418 in the Cisco Unified Communications Manager Administration Guide.

Note

Remote-Party-ID (RPID) headers coming in from the SIP gateway can interfere with QSIG content and cause unexpected behavior with Call Back capabilities. To prevent interference with the QSIG content, turn off the RPID headers on the SIP gateway.

When you create a SIP trunk with Cisco Intercompany Media Engine (IME) selected as the trunk service type, the default for the Tunneled Protocol field is QSIG. QSIG must be the tunneled protocol for QSIG features to work on a Cisco IME trunk.

Note

Cisco Unified Communications Manager supports only connection retention mode for Call Back on an a Cisco IME trunk.

SIP PUBLISH

SIP PUBLISH provides the preferred mechanism for Cisco Unified Communications Manager Release 6.0 (and later) to send IP phone presence information to Cisco Unified Presence Release 6.0 (and later) over a SIP trunk because it provides improved performance. PUBLISH also provides presence information on a line basis; for example, for do not disturb and mobility. Only outbound PUBLISH gets supported. (Cisco Unified
Communications Manager Release 6.0 [and later] uses SUBSCRIBE/NOTIFY for presence when communicating to Cisco Unified Presence release 1.0.

PUBLISH represents a SIP method for event state publication. RFC 3903 provides a framework for the publication of event state from a user agent to an entity that is responsible for the composition of this event state and distributing it to interested parties through the SIP Events framework. The mechanism that is described in RFC 3903 can extend to support publication of any event state for which an appropriate event package exists.

In addition, RFC 3903 defines a concrete usage of that framework for the publication of presence state by a presence user agent to a presence compositor.

SIP trunk works with Cisco Unified Presence to provide the presence information for the Cisco Unified Communications Manager registered phones. In release 5.0, Cisco Unified Presence collected the presence information from Cisco Unified CallManager through the SIP subscription mechanism.

The Cisco Unified Communications Manager to Cisco Unified Presence interaction works properly when the SIP subscription mechanism is used; however, this mechanism brings some performance concerns. Both Cisco Unified Communications Manager and Cisco Unified Presence must maintain a separate subscription dialog for each phone that is being watched. Moreover, if a phone is interested by two different users, and each user has a different watch rule, Cisco Unified Presence will issue two different SUBSCRIBE requests to the Cisco Unified Communications Manager SIP trunk for the same number.

In Cisco Unified Communications Manager Release 6.0 (and later), a SIP trunk can use PUBLISH as the mechanism for the presence interaction with Cisco Unified Presence. Cisco Unified Communications Manager acts as the Event Publication Agent (EPA), publishing the presence information of its managed phones; Cisco Unified Presence acts as the Event State Compositor (ESC), receiving the published presence information, aggregating it, and updating the watcher phone displays accordingly.

**Cisco Unified Communications Manager and Cisco Unified Presence high-level architecture overview**

The figure below shows how Cisco Unified Communications Manager, Cisco Unified Presence, and Cisco Unified IP Phones work together.

- Cisco Unified Communications Manager manages all the IP phones, and Cisco Unified Communications Manager uses the SIP or SCCP interface to control the phones.
- An HTTP interface also exists between the IP phones and Cisco Unified Presence. This interface gets used for Cisco Unified Presence to update phone screens. It also gets used for Cisco Unified Presence to detect user login/logout activities.
• The SIP trunk interface gets used to pass the presence data between Cisco Unified Communications Manager and Cisco Unified Presence.

**Figure 43: SIP PUBLISH High-Level Architecture**

Cisco Unified Communications Manager Administration Configuration Tips for PUBLISH

The following configuration tips apply to Cisco Unified Communications Manager Administration when a SIP trunk is configured for PUBLISH:

• From the SIP Trunk Configuration window, configure a SIP trunk to access the Cisco Unified Presence (destination address).

**Tip**

To maximize the distributed performance in a multinode cluster, Cisco recommends that you configure the SIP trunk to use the default device pool.

• From the Service Parameters Configuration window for the Cisco CallManager service, in the CUP PUBLISH Trunk field, choose the SIP trunk that you configured.

• Configure a Cisco Unified Presence end user (User Management > End User Configuration) and assign a licensing unit to the user (System > Licensing > Capabilities Assignment).

• Associate the end user with the line appearance (Device > Phone Configuration). From the Phone Configuration window, click the DN that the user will use to access the Cisco Unified Presence. Click the Associate End Users button. From the Find and List Users window, choose an end user that will access the Cisco Unified Presence.

**Note** You can associate one line appearance with up to five end users.

• DND Support for SIP Trunk PUBLISH-Because DND is device based in release 6.0 (and later), if a device is changed to the DND state, all Cisco Unified Presence-enabled line appearances that are associated with this device could get published. When a device gets changed to the DND state, DND as well as the busy/idle status will get published together to give Cisco Unified Presence more flexibility to process the data.

• Shared Lines-If Phone A and Phone B are sharing DN 1000, when a user picks up Phone A and makes a call on the line 1000, Cisco Unified Communications Manager notifies Cisco Unified Presence that...
line 1000 is busy. This information gives the watcher the illusion that all lines for DN 1000 are busy. This does not represent accurate information because line 1000 on Phone B remains idle. Cisco Unified Communications Manager tells Cisco Unified Presence that line 1000 on Phone A is busy. In release 6.0 (and later), Cisco Unified Communications Manager publishes by line appearance. The system considers a line appearance a (DN, Device) pair.

- Multiple Partitions-When Cisco Unified Communications Manager publishes the presence status of a DN, it also shows the partition in which the DN is associated.

- Associating Username-With shared line and multiple partitions supported, Cisco Unified Presence cannot assume that it works only with one DN for each phone and also one partition across the whole Cisco Unified Communications Manager system. In release 6.0 (and later), because a line appearance can be associated with an end user, a SIP trunk will publish the status of the line appearance on behalf of the end user that is associated with that line appearance, which means it can get used to identify Cisco Unified Presence-enabled lines. If a line appearance is associated with an end user, the system is considered as Cisco Unified Presence-enabled; therefore, its presence information will get published.

**Service Parameters for PUBLISH**

The following Cisco CallManager service parameters get used to configure PUBLISH:

- CUPS PUBLISH Trunk
- Default PUBLISH Expiration Timer
- Minimum PUBLISH Expiration Timer
- Retry Count for SIP Publish
- SIP Publish Timer

**Serviceability Performance Counters**

Cisco Unified Serviceability collects and displays the following PUBLISH-related performance counters:

- SIP_StatsPublishIns
- SIP_StatsPublishOuts
- SIP_StatsRetryPublishOuts
- SIP_StatsRetryRequestsOut

The following performance counters exist in Cisco Unified CallManager Release 5.x, but the PUBLISH feature impacts their values:

- SIP_SummTotalOutReq
- SIP_SummTotalInRes
- SIP_StatsRetryRequestsOut

**Security Recommendations**

RFC 3903 suggests the use of TLS and digest authentication against issues such as Access Control, Denial of Service Attacks, Replay Attacks, and Man in the Middle Attacks. Because Cisco Unified Communications Manager and Cisco Unified Presence support TLS and digest authentication, no changes occurred in release
6.0. The administrator can configure and enable TLS and digest authentication for Cisco Unified Communications Manager and Cisco Unified Presence. Additionally, you can use IPSec as an alternative to TLS.

**BAT Support**

The following BAT tools assist in migrating Cisco Unified Presence users to Cisco Unified Communications Manager:

- BAT provides a tool that examines all Cisco Unified Presence licensed users and their primary extensions and associated device line appearances for users after Cisco Unified Communications Manager is upgraded from 5.x to 6.0 (and later). You need this tool during the upgrade/migration of Cisco UnifiedPresence when connecting to Cisco Unified Communications Manager (because all the backend subscriptions get deleted and the new line appearance-based presence needs to be available for the Cisco Unified Presence users). To perform the migration, BAT uses the Export and Update functions. The export csv format follows: UserID, Device, Directory Number, Partition. The last three columns form a line appearance.

- To access the Export and Update windows, choose **Bulk Administration > Users > Export Line Appearance** and **Bulk Administration > Users > Line Appearance > Update Line Appearance**.

- The Export and Update windows include a check box, Export Line Appearance for CUP User Only (and Update Line Appearance for CUP Users Only). When this check box gets checked, the export or update operation gets performed on the Cisco Unified Presence users. Non-Cisco Unified Presence users do not get exported or updated.

**SIP OPTIONS**

In Cisco Unified Communications Manager, the SIP OPTIONS method allows a SIP trunk to track the status of remote destinations. By sending outgoing OPTIONS and checking the incoming response message, the SIP trunk knows whether remote peers are ready to receive a new request. The SIP trunk does not attempt to set up new calls to unreachable remote peers; this approach allows for quick failovers.

Cisco Unified Communications Manager uses SIP OPTIONS as a keep-alive mechanism on the SIP trunk. Cisco Unified Communications Manager periodically sends an OPTIONS request to the configured destination address on the SIP trunk. If the remote SIP device fails to respond or returns a SIP error response, Cisco Unified Communications Manager tries to reroute the calls by using other trunks or by using a different address, depending on the configuration.

The OPTIONS request lies outside the context of a call; therefore, the request allows Cisco Unified Communications Manager to detect failures even if no calls are present on the SIP trunk. This approach allows any subsequent calls to be rerouted more quickly. The SIP OPTIONS method prevents calls from incurring large timeout and retry delays before the calls get rerouted.

**Cisco Unified Communications Manager Configuration Tips**

The following configuration tips apply to Cisco Unified Communications Manager Administration when a SIP trunk is configured for OPTIONS:

- Configure a SIP profile to enable SIP OPTIONS. (Use the **Device > Device Settings > SIP Profile** menu option in Cisco Unified Communications Manager Administration.) Copy the Standard SIP Profile and rename the copy; for example, OPTIONS Profile. Check the **Enable OPTIONS Ping to monitor**
destination status for trunks with service type “None (Default)” check box. SIP OPTIONS is disabled by default.

- From the SIP profile that you created, update the two request timers if necessary. One timer gets used when the SIP trunk is in service or partially in service; the second timer gets used when the SIP trunk is out of service. Cisco Unified Communications Manager initiates the SIP OPTIONS requests to the configured destination address(es) of the SIP trunk by using the configured transport protocol (for example, UDP or TCP).

**Note**

When the request timers expire, Cisco Unified Communications Manager checks whether it has received responses to all previously sent OPTIONS requests. Cisco Unified Communications Manager does not send any new OPTIONS requests if it is still waiting for responses to previous OPTIONS requests. Thus, the system does not burden the network with multiple concurrent OPTIONS requests.

- From the SIP profile that you created, set the SIP OPTIONS retry timer and counter.
- Configure a SIP trunk (if one is not already configured). The trunk service type of the SIP trunk must specify None (default). Dynamic SIP trunks, such as Call Control Discovery, Extension Mobility Cross Clusters, and Intercompany Media Services, are not supported.
- Use Trunk Configuration to configure the destination information. Multiple destinations can be configured. If the destination address is configured as a host name (instead of a dotted IP address), and multiple addresses are returned, the system sends OPTIONS messages to the returned addresses until a response is received. If no response is received before all returned addresses have been exhausted, the SIP trunk gets marked as “target in down state.”

**Note**

For SIP trunks, Cisco Unified Communications Manager supports up to 16 IP addresses for each DNS SRV and up to 10 IP addresses for each DNS host name. The order of the IP addresses depends on the DNS response and may be identical in each DNS name. The OPTIONS request may go to a different set of remote destinations each time if a DNS SRV record (configured on the SIP trunk) resolves to more than 16 IP addresses, or if a host name (configured on the SIP trunk) resolves to more than 10 IP addresses. Thus, the status of a SIP trunk may change because of a change in the way a DNS query gets resolved, not because of any change in the status of any of the remote destinations.

- Assign the SIP profile that has OPTIONS Ping enabled to the SIP trunk.

When the destination of a SIP trunk includes or resolves to more than one IP address, call routing uses a random selection algorithm to select the destination IP address for the next call on a SIP trunk. If SIP OPTIONS is enabled for the trunk, the state information for the selected IP address determines whether to send the INVITE or advance to the next destination.

**SIP OPTIONS and Secure SIP Trunks**

The SIP OPTIONS method supports secure SIP trunks for which the Transport Type setting specifies TLS in the SIP trunk security profile. Unlike other requests or responses (such as INVITE), Cisco Unified Communications Manager does not verify the X.509 Subject Name setting (configured in the SIP trunk security profile) for OPTIONS requests or responses. So, a remote destination can be marked as available based on OPTIONS request or response, but the call setup request (such as INVITE) may fail with a reason code 403.
Forbidden. Misconfiguration of the X.509 Subject Name at either the Cisco Unified Communications Manager that sends the OPTIONS request or at the Cisco Unified Communications Manager that receives and responds to the OPTIONS request may cause this failure.

Consider the following two scenarios.

**Scenario 1**
Unified CM 1 sends an OPTIONS request over a SIP trunk to Unified CM 2 and receives a 200 OK response. The X.509 Subject Name in the SIP trunk security profile is misconfigured at Unified CM 2; therefore, Unified CM 2 gets marked as available at Unified CM 1. When the INVITE gets sent from Unified CM 1 to Unified CM 2, Unified CM 2 sends a 403 Forbidden message to Unified CM 1. The following figure illustrates this scenario.

*Figure 44: X.509 Subject Name Verification Failure at Destination*

**Scenario 2**
Unified CM 1 sends an OPTIONS request over a SIP trunk to Unified CM 2 and receives a 200 OK response. Unified CM 1 marks Unified CM 2 as available, although the X.509 Subject Name in the SIP trunk security
profile is misconfigured at Unified CM 1. In this case, the INVITE request from Unified CM 1 to Unified CM 2 fails. The following figure illustrates this scenario.

**Figure 45: X.509 Subject Name Verification Failure at Source**

![Diagram](https://example.com/diagram.png)

**SIP OPTIONS and Digest Authentication**

When digest authentication is enabled for a SIP trunk (the Enable Digest Authentication check box is checked in the corresponding SIP trunk security profile), the remote destination gets marked as available upon receipt of a 401 (Unauthorized) response for the OPTIONS request. After receipt of a 401 response, OPTIONS is resent with the digest credentials; upon credential verification from the remote side, a 200 OK response is received for the OPTIONS request.

For an OPTIONS request where the SIP realm (upon receipt of an initial 401 response) or digest credentials are mismatched (remote side), any subsequent INVITE requests fail, even though the remote destination is marked as available.

**Serviceability Alarms**

The following alarms support SIP OPTIONS:

- SIPTrunkOOS
- SIPTrunkPartiallyISV
- SIPTrunkISV

**SIP early offer**

To enhance interoperability with third-party SIP devices, Cisco Unified Communications Manager allows you to configure SIP trunks to enable early offer for outgoing voice and video calls without requiring MTP, if media capabilities and media port information of the calling endpoint is available.

**Outgoing Call Setup**

For outgoing call setup for an early offer trunk, Cisco Unified Communications Manager includes an SDP with the calling device media port, codecs, and IP address of the calling device (when available); inserts an MTP for early offer only when the media information for the caller is unavailable; and advertises multiple
codecs when an MTP that supports multiple codecs gets inserted. In previous releases, Cisco Unified Communications Manager provided early offer SDP only when administrators enabled MTP Required or E2E RSVP on the outgoing SIP trunk. The early offer feature ensures that a higher percentage of outbound early offer SIP trunk calls get made without requiring an MTP, thus reducing the number of MTP resources that are needed and improving interoperability with third-party PBXs.

Cisco Unified Communications Manager supports early offer (without requiring MTP) when one of the following devices initiates the call:

- SIP phones
- SCCP phones with SCCP v20 support, which provides media port information through the getPort capability
- MGCP gateways
- Incoming H323 fast start calls
- Incoming early offer SIP trunk calls

For endpoints where the media port information is not available (for example, H323 slow start calls or delayed offer SIP calls or legacy SCCP phones), Cisco Unified Communications Manager still allocates an MTP to provide SDP in the initial INVITE.

For calls that any of the devices in the preceding list initiate, MTP may be needed due to other reasons, such as DTMF/codec mismatch, TRP required on the inbound or outbound trunk, or MTP required on the calling side.

Mid-Call Setup

Cisco Unified Communications Manager also enhances interoperability with third-party devices during mid-call operations, such as basic hold/resume operations, and during supplementary services, such as transfer and conference. In previous releases, Cisco Unified Communications Manager sent an INVITE with an inactive SDP (a=inactive attribute) to indicate a break in media path, sent a delayed offer INVITE to insert music on hold or to resume the media stream, and expected a send-recv offer SDP in the 200 OK. Because third-party devices often provide an inactive offer SDP in the 200 OK instead of providing a send-recv offer SDP, the media path remains in an inactive state and causes calls to drop.

Cisco Unified Communications Manager allows you to configure a parameter for an early offer SIP trunk so that Cisco Unified Communications Manager suppresses the sending of inactive or sendonly SDP in mid-call INVITEs. When this parameter gets enabled, Cisco Unified Communications Manager connects the SIP trunk device directly to the MOH or announciator device without breaking the existing media stream during call hold or during other feature invocation. Similarly, Cisco Unified Communications Manager connects the SIP trunk device to a line-side device directly during call resume without breaking the MOH or announciator stream. By preventing the far-end media stream from getting set to inactive, Cisco Unified Communications Manager should always be able to resume the media path.
You should configure the suppression of inactive or send only SDP only if you experience interoperability issues with third-party SIP devices during hold-resume or during media resumption for supplementary services. Certain endpoints, such as Cisco Unity Connection, may not work if you enable this configuration.

Get Port Capability Support

Cisco Unified Communications Manager also provides a send-receive SDP in response to a delayed offer invite in an initial call or mid-call on a SIP trunk if the device that connects to a SIP trunk supports the GetPort capability. Cisco Unified Communications Manager provides this functionality regardless of whether the SIP trunk has been configured for early offer. If the device does not support the GetPort capability, Cisco Unified Communications Manager does not insert another MTP to provide a send-receive offer.

If you want to change the amount of time that Cisco Unified Communications Manager waits to receive the audio/video/data port from the SCCP device or MTP after the call is connected, you can configure the Port Received Timer After Call Connection service parameter. If Cisco Unified Communications Manager fails to receive the video port before the time specified in this parameter elapses, the call is initially established with two-way audio only. Two-way video may be established after another offer/answer transaction gets completed. If Cisco Unified Communications Manager fails to receive the audio port before the time specified in this timer expires, Cisco Unified Communications Manager attempts another offer/answer transaction to establish a two-way media path for both audio and video.

Increasing the timer allows more time for Unified CM to receive the port information but may result in delayed audio/video at the start or during the call. If the calling device is a CTI or Unified Video Advantage application using CAST protocol version 3, you may need to adjust the timer to accommodate the time that the application needs to open the connection and get the port information.

Early offer limitations and interactions

The following limitations and interactions apply to the early offer feature:

- The early offer feature requires that your MTP uses IOS version 15.1(2)T or later.
- SRTP and video—Cisco Unified Communications Manager can advertise secure audio and/or video capabilities in the SDP of an initial INVITE, depending on the capabilities of calling device.
- End-to-end (E2E) RSVP—Because E2E RSVP provides an early offer by including an SDP in the initial INVITE, the early offer and E2E RSVP features are mutually exclusive in the SIP Profile Configuration window. When you choose E2E from the RSVP Over SIP drop-down list box, the Early Offer support for voice and video calls (insert MTP if needed) check box gets disabled.
- Single Number Reach (SNR)—When a call gets initiated to trunk single number reach (SNR) destinations from a SIP phone, SCCP v20 phone, or calling device whose media capabilities are available at setup, the INVITE SDP contains the IP address and port of the calling device. When an MTP is required to provide early offer for SNR trunk calls, a separate MTP port gets allocated for each SNR destination.
- IPv6—Cisco Unified Communications Manager sends delayed offer INVITEs for the following IPv6 scenarios, even if you have configured early offer on a SIP trunk:
  - SIP trunk is configured in IPv6 only mode.
  - Calling device is in IPv6 only mode.
  - SIP trunk is in dual mode and ANAT is enabled.
- SIP trunk is in dual mode and Media Address Preference is IPv6.

- For the delayed offer SIP call to early offer interworking case, Cisco Unified Communications Manager inserts an MTP to provide SDP on the outgoing call leg. The INVITE contains audio lines only. The INVITE that is sent on the outgoing leg includes audio media lines only. The calling video capabilities and cryptographic key of the device are not available to the tandem cluster; thus, no cryptographic attribute for audio or video media line exists. As a result, the outgoing INVITE SDP contains the IP and audio port of the MTP and no SRTP key or attributes in the audio media line and no video media lines.

- For the slow start H323 calls to early offer interworking case, Cisco Unified Communications Manager inserts an MTP to provide SDP on the outgoing call leg. The INVITE contains audio lines only. The INVITE sent on the outgoing leg includes audio media lines only. The calling video capabilities and cryptographic key of the device are not available to the tandem cluster; thus, no cryptographic attribute for audio or video media line exists. As a result, the outgoing INVITE SDP contains the IP and audio port of the MTP and no SRTP key or attributes in the audio media line and no video media lines. Cisco Unified Communications Manager escalates to video after it receives video TCS from H323 leg after media cut-through and if call admission control (CAC) allows video and the allocated MTP supports pass-through and multimedia.

- Cisco Unified Communications Manager sends delayed offer INVITEs for the following scenarios:
  - Mid-call media renegotiation
  - Call hold-Cisco Unified Communications Manager sends a delayed offer INVITE in mid-call when inserting MOH, because the MOH server might not support the same codec as the negotiated audio call. Cisco Unified Communications Manager needs the complete codec list from the far end to renegotiate media.
  - Call resume

  **Note**

  When a line-side device initiates a call transfer and leaves the call, Cisco Unified Communications Manager connects one or two trunk legs and sends a delayed offer INVITE in mid-call. Using a delayed offer INVITE ensures that features, such as video and SRTP, do not get dropped when transfers result in two trunk call legs getting connected.

- Cisco Unified Communications Manager sends a delayed offer INVITE or outgoing call fails when one of the following situations occurs:
  - If an allocated MTP, transcoder, or TRP does not support getPort capability and an outbound SIP trunk leg is enabled for early offer, Cisco Unified Communications Manager does not allocate another media resource to provide early offer.
  - When the Use Trusted Relay Point setting is enabled on a SIP trunk (Device > Trunk) and the allocated media resource does not support TRP capability or fails to provide the media port, Cisco Unified Communications Manager does not allocate another media resource. This situation can occur if the MTP or RSVP Agent is not configured for TRP.
  - Depending on the setting of the Fail Call If MTP Allocation Fails service parameter or the Fail Call If TRP Allocation Fails service parameter, Cisco Unified Communications Manager sends a delayed offer or fails the call.
• Configure UPDATE and PRACK on the SIP trunk to provide ringback in blind transfer cases when the consult call leg on early offer SIP trunk provides inband ringback or announcements. If the trunk is not enabled for PRACK or if the far-end device does not support UPDATE, the transeree does not receive a ringback tone.

• As in previous releases, you cannot change the codec order in the offer SDP. Cisco Unified Communications Manager orders the codecs based on an internal list, typically from highest to lowest. To work around this issue, you can create a SIP Normalization script to reorder the codecs in the offer SDP.

Traces

The following examples show the traces that help you troubleshoot early offer calls.

SIP Trunk Trace

001685280 |2010/05/25 13:50:31.980 |100 |AppInfo |||SIPCdpc(1,100,67,9)|1,100,67,9.1^*^*|//SIP/SIPCdpc(1,67,9)/ci=30801944/c sbId=0/StartTransition: requireInactiveSDPForMidcallMediaChange=0, isTrunkEnabledForVoiceEO=1

Note

1 indicates early offer is enabled for this call; 0 indicates that early offer is disabled.

001685289 |2010/05/25 13:50:32.001 |100 |SdlSig |PolicyAndRSVPRegisterReq |wait |RSVPSessionMgr(1,100,91,1) |SIPCdpc(1,100,67,9) |1,100,49,1.100206^172.18.199.61^SEP001319ACCA00 |[R:N-H:0,N:0,L:0,V:0,2:0,D:0] CI= 30801944 Branch= 0 reg=Default cap=0 loc=0 MRGLPkid=1d1ba42-9575-e3dc-ba78-fbl1d56db546 PrecLev=5 VCall=F VCapa=F VCapCount=0 regiState=0 medReq=0 dataCapFl=2 IsEmccD=F EmccDName=to-ccm84 rcId= ipMode=0 eoType=2 getPort=F sRTP=F cryptocap=0 tm=16 DTMF(wantRecep=1 provOOB=1 suppMeth=1 Cfg=1 PT=0 reqMed=0) hInCodec=F distMed=F mediaEP=F rsvpQoSType=0 qosFallback=F status=0 sipOfferNeededInd=T hasSDP=F geolocInfo={geolocPkid=, filterPkid= geoilocVal=}, devType=8

Note

The values for eoType include the following: None (0), early offer for G.Clear (1), early offer for voice and video (2), and early offer for G.Clear voice and video (3).

001685353 |2010/05/25 13:50:32.087 |100 |SdlSig |PolicyAndRSVPRegisterRes |outCall waitRSVPRes |SIPCdpc(1,100,67,9) |RSVPSession(1,100,93,5) |1,100,49,1.100207^172.18.199.61^SEP001319ACCA00 |[R:N-H:0,N:0,L:0,V:0,Z:0,D:0] CI=...
30801944 Branch= 0 Status=1 rsvpPol=1 vCall=F e2eRSVPInserted=F eoStatus=1 hasSDPMsg=T
RSVPagent: confID =0 ci =0 capCt =0 reg= mtpType =2 agentCt =0 agentAllo=0 RemoAgent=F
DevCap=0 ipAddrMode=0

The valid values for eoStatus include the following: None(0), early offer for voice and video (1), early offer for G.Clear (2), Continue delayed offer (3), and failed call (4).

---

**Trace for StationD (SCCP Device) That Participates in an Early Offer Call**

001685325 |2010/05/25 13:50:32.064 |100 |SdlSig |DeviceMediaInfoReq
|restart0
|StationD(1,100,50,13) |RSVPSession(1,100,93,5)
|1,100,49,1.100206^172.18.199.61^SEP001319ACCA00
|\[R:N-H:0,N:0,L:0,V:0,Z:0,D:0\] CI=
30801943 confID=30801943 callRefID=30801943 counter=1 mediaType=1 iptype=0
PPID=16777217 regCode=1
001685327 |2010/05/25 13:50:32.064 |100 |SdlSig |StationPortReq |restart0
|StationD(1,100,50,13) |StationCdpc(1,100,51,1)
|1,100,49,1.100206^172.18.199.61^SEP001319ACCA00
|\[R:N-H:0,N:0,L:0,V:0,Z:0,D:0\] confID=30801943 PPID=16777217 CI=30801943 transportType=1 addrType=0
mediaType=1 .

Response from the SCCPv20 device:

001685328 |2010/05/25 13:50:32.081 |100 |AppInfo
|\|\|\|StationInit(1,100,49,1)|1,100,49,1.100207^172.18.199.61^SEP001319ACCA00|StationInit:
\(0000013\) PortRes IpAddr=0x399eb00, Port=31780, RTCPPort=0, confID=30801943, PPID=16777217
001685330 |2010/05/25 13:50:32.081 |100 |SdlSig |StationPortRes
|outgoing_call_proceeding3
|StationCdpc(1,100,51,1) |StationD(1,100,50,13)
|1,100,49,1.100207^172.18.199.61^SEP001319ACCA00
|\[R:N-H:0,N:0,L:0,V:0,Z:0,D:0\] CI=
30801943 confID=30801943 ptpID=16777217 ipaddr=0x\{ac,12,c7,3d,0,0,0,0,0,0,0,0,0,0,0\}
port=31780 .type=0. RTCPPort=0 mediaType=1
001685331 |2010/05/25 13:50:32.082 |100 |SdlSig |DeviceMediaInfoRes |wait
|RSVPSessionMgr(1,100,91,1) |StationCdpc(1,100,51,1)
|1,100,49,1.100207^172.18.199.61^SEP001319ACCA00
|\[R:N-H:0,N:0,L:0,V:0,Z:0,D:0\] CI=
30801943 confID=30801943 callRefID=30801943 mediaType=1 iptype=0
PPID=16777217 regCode=1
port=31780 RTCPPort=0 ipAddrType=0 ipv4=172.18.199.61 status=0
Media Layer Trace for Early Offer Call When MTP Allocation Is Required

001686458 |2010/05/25 13:50:48.535 |100 |SdlSig |AuEarlyOfferConnectReq |waitForAll |MediaCoordinator(1,100,125,1) |RSVPSession(1,100,93,6) |1,100,49,1.100222^172.18.201.82^SEP0014F2E982F1 |[R:N=H:0,N:0,L:0,V:0,Z:0,D:0] Party1: CI=30801945 capCount=7 region=Default xferMode=4 mrid=0 audioId=0 videoCap=F dataCap=2 activeCap=0 cryptoCapCount=0 flushIns=0 dtmCall=0 dtmPrimaryCI=0 IFPid=(0,0,0,0) dtMedia=F honorcodec=F EOType=0 MohType=0 Party2: CI=30801946 capCount=0 region=Default xferMode=16 mrid=0 audioId=0 videoCap=F dataCap=2 activeCap=0 cryptoCapCount=0 flushIns=0 dtmCall=0 dtmPrimaryCI=0 IFPid=(0,0,0,0) dtMedia=F honorcodec=F EOType=2 MohType=0 videoCall=F confID =0 ci =0 capCt =0 reg= mtpType =2 agentCt =0 agentAllo =0 RemoAgent=F DevCap=0 ipAddrMode=0 mtpInsReason=32 hasSDP=F

---

Note: Valid values for mtpInsReason include the following: None (0), TRP Side B (1), TRP Side A (2), Transcoder Side A (4), MTP Side A (8), DTMF mismatch (16), early offer (32).

---

001686676 |2010/05/25 13:50:48.646 |100 |SdlSig |AuEarlyOfferConnectReply |wait |RSVPSession(1,100,93,6) |MediaCoordinator(1,100,125,1) |1,100,49,1.100223^172.18.197.154^MTP_sinise |[R:N=H:0,N:0,L:0,V:0,Z:0,D:0]

|ciParty1=30801945 |ciParty2=30801946 |devicePidParty1=(1,100,50,3) |devicePidParty2=(1,100,67,10) |err=0 |videoFlag=F |hasSDP=F.

---

Note: Valid values for Err codes for media resource allocation failures include the following: No Error (0), TRP allocation Side B (1), TRP Side A (2), Transcoder Side A (3), MTP Side A (4), MTP for DTMF mismatch (5), MTP for early offer (6).

---

Troubleshooting early offer issues

For assistance in troubleshooting early offer problems, see the following table.
### Table 39: Troubleshooting Early Offer Problems

<table>
<thead>
<tr>
<th>Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>The initial outgoing INVITE for an early offer SIP trunk call does not contain an SDP.</td>
<td>1   Verify that you checked the Enable Early Offer for voice and video calls check box on the SIP associated with the early offer trunk.</td>
</tr>
<tr>
<td></td>
<td>2   Verify that the SIP trunk is not in IPv6 only mode or dual-mode trunk with ANAT or media preference set to IPv6.</td>
</tr>
<tr>
<td></td>
<td>3   Verify that calling device is not an IPv6-only device.</td>
</tr>
<tr>
<td></td>
<td>4   If initiating calls from pre SCCP v20 device or H323 Slowstart device or if this is a delayed offer incoming call, verify that MTP allocation is taking place.</td>
</tr>
<tr>
<td></td>
<td>5   Ensure that the caller or SIP trunk media resource group list has an MTP available. Verify that the MTP firmware supports getPort capability. If the MTP image does not support getPort capability, upgrade to a newer image, IOS release 15.1(2)T or later.</td>
</tr>
<tr>
<td></td>
<td>6   For an SCCP v20 calling device, verify that the device provides the media port in StationPortRes/DeviceMediaInfoRes. If not, check for a timeout event-GetPortResponseTimer or TimeoutWaitingForPortInfo.</td>
</tr>
<tr>
<td>Problem</td>
<td>Solution</td>
</tr>
<tr>
<td>---------</td>
<td>----------</td>
</tr>
</tbody>
</table>
| An outgoing call for an early offer SIP trunk fails. Cisco Unified Communications Manager does not send an INVITE. | 1 If initiating calls from pre-SCCP v20 devices or H323 slowstart or delayed offer incoming trunk, verify that MTP allocation takes place and that the MTP supports SCCP v20.  
2 If the MTP allocation fails, do one or more of the following:  
   • Check the configuration for the Fail Call Over SIP Trunk If MTP Allocation Fails service parameter and set it to False.  
   • Include an MTP in the media resource group list that associates with the SIP trunk or default pool.  
3 If the MTP image does not support getPort capability, upgrade to a newer image, IOS release 15.1(2)T or later.  
4 If initiating calls from SCCP v20 devices, check whether Cisco Unified Communications Manager times out (typically after 2 seconds) while waiting for StationPortRes from the SCCP line device. If so, the SCCP device needs to be reset or phone logs need to be collected. Also, check the configuration of the Fail Call Over SIP Trunk If MTP Allocation Fails service parameter. If you want Cisco Unified Communications Manager to send a delayed offer invite, set the parameter to False. |

The outgoing call for early offer SIP trunk always has SDP with one codec and the IP address and port of the MTP. | 1 Verify that the Media Termination Required check box is not checked in the Trunk Configuration window for this trunk.  
2 If the Media Termination Required check box is not checked on the Trunk Configuration window for this trunk, check whether a media resource is being allocated. Media resources can get allocated for local RSVP, TRP enabled on trunk, early offer, DTMF mismatch, or codec mismatch.  
3 Verify that the media resource is configured for pass-through codec. |
<table>
<thead>
<tr>
<th>Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>There is no video during initial call when MTP is inserted in the call.</td>
<td>1  Verify that the Media Termination Required check box is not checked in the Trunk Configuration window for this trunk.</td>
</tr>
<tr>
<td></td>
<td>2  Verify that Cisco Unified Communications Manager MTP is not allocated. The Cisco Unified Communications Manager MTP does not support video pass-through.</td>
</tr>
<tr>
<td></td>
<td>3  If an IOS MTP is allocated, verify that the IOS MTP is configured with pass-through codec. IOS MTP supports video pass-through.</td>
</tr>
<tr>
<td></td>
<td>4  Verify that location call admission control allows a video call.</td>
</tr>
<tr>
<td>Call is not secured when MTP is inserted in the call.</td>
<td>1  Verify that the Media Termination Required check box is not checked in the Trunk Configuration window for this trunk.</td>
</tr>
<tr>
<td></td>
<td>2  Verify that the IOS MTP is configured with pass-through codec.</td>
</tr>
<tr>
<td></td>
<td>3  Verify that call does not initiate from H323 slowstart device or delayed offer trunk.</td>
</tr>
</tbody>
</table>

**Cisco Unified Communications Manager SIP endpoints overview**

The Cisco Unified IP Phones 7911, 7941, 7961, 7970, and 7971 get deployed as a SIP endpoint in a Cisco Unified Communications Manager Back to Back User Agent (B2BUA) environment. The SIP provides the primary interface between the phone and other network components. In addition to SIP, other protocols get used for various functions such as DHCP for IP address assignment, DNS for domain name to address resolution, and TFTP for downloading image and configuration data.

This section provides an example illustration and brief description of the B2BUA and peer-to-peer environments.
Cisco Unified Communications Manager Business Edition 5000 does not support the following example.

Note

The above shows a simplified example of a Cisco Unified Communications Manager B2BUA network that shows a main site and a branch office deployment. Each site includes a mixture of phones that are running SIP and phones that are running SCCP. The main site contains the Cisco Unified Communications Manager cluster and voice mail server. Each phone at the main site and the branch office site homes to a set of primary, secondary, and tertiary Cisco Unified Communications Managers. This provides redundancy of call control in the event of the failure of an individual Cisco Unified Communications Manager server.

Phones that are running SIP that are at the main site direct all session invitations to Cisco Unified Communications Manager. Based on routing configuration and destination, Cisco Unified Communications Manager will either extend a call locally to another phone that is running SIP or phone that is running SCCP, through the main site voice gateway across the IP WAN to one of the phones in the branch office, or through the main site voice gateway to the PSTN. Calls that are originating from phones in the branch office get routed similarly with the added ability of routing calls to the PSTN through the branch office voice gateway.

The branch office includes an SRST gateway that is deployed for access to the main site IP WAN and for PSTN access. Phones that are running SIP in the branch office will direct all session invitations to the Cisco Unified Communications Manager at the main site. Similarly to the phones at the main site, Cisco Unified Communications Manager may extend the call to a phone at the main site, through the main site voice gateway across the IP WAN to a phone in the branch office, or to the PSTN. Depending on the routing configuration of the Cisco Unified Communications Manager cluster, PSTN calls that originate from the phones in the branch office can get routed to the PSTN through the gateway at the main site, or they can be routed locally to the PSTN through the branch office gateway.

The SRST gateway also acts as a backup call control server in the event of an IP WAN outage. Both the phones that are running SIP and phones that are running SCCP will fail over to the SRST gateway during a
WAN failure. By doing so, the phones in the branch office can have their calls routed by the SRST gateway. This includes calls that originate and terminate within the branch office and calls that originate and terminate in the PSTN.

**Related Topics**

[SIP trunk, on page 453](#)

---

**SIP line side overview**

The SIP line side feature affects Cisco Unified Communications Manager architecture, the TFTP server, and the Cisco Unified IP Phones. The phone features of the phone that is running SIP, which are equivalent to the phone features of the phone that is running SCCP, behave similarly. Cisco Unified IP Phones 7941/61/71/70/11 support all features and most CTI applications. Cisco Unified IP Phones 7905/12/40/60 support a reduced feature set (for example, limited MOH and failover capabilities). SIP trunk side applications work for both phones that are running SCCP and phones that are running SIP.

**SIP standards**

The SIP standards described in this section are supported in Cisco Unified Communications Manager.

**RFC3261 RFC3262 (PRACK) RFC3264 (offer/answer) RFC3311 (UPDATE) 3PCC**

This SIP standard supports the following Cisco Unified Communications Manager features:

- Basic Call
- Hold and Resume
- Music on Hold
- Distinctive Ringing
- Speed dialing
- Abbreviated Dialing
- Call Forwarding (for example, 486 and 302 support)
- Meet-Me
- Pickup, Group Pickup, Other Group Pickup
- 3-way calling (local mixing of phone that is running SIP)
- Parked Call Retrieval
- Shared line: Basic Call

**RFC3515 (REFER) also replaces and referred-by headers**

These SIP standards support the following Cisco Unified Communications Manager features:

- Consultative Transfer
• Early Attended Transfer
• Blind Transfer

Remote Party Id (RPID) header
This SIP standard supports the following Cisco Unified Communications Manager features:
• Calling Line ID (CLID)
• Calling Party Name ID (CNID)
• Dialed Number ID Service (DNIS)
• Call-by-call Calling Line ID Restriction (call-by-call CLIR)

RPID represents a SIP header that is used for identification services. RPID indicates the calling, called, and connected remote party information to the other party for identification and callback, legal intercept, indication of user identification and user location to emergency services, and the identification of users for accounting and billing services.

Diversion header
This SIP standard supports the following Cisco Unified Communications Manager features:
• Redirected Number ID Service (RDNIS)
• Call Forward All Activation, Call Forward Busy, Call Forward No Answer

Replaces header
This SIP standard supports the following Cisco Unified Communications Manager feature:
• Shared Line: Remote Resume

Join header
This SIP standard supports the following Cisco Unified Communications Manager feature:
• Shared Line: Barge

P-Charging-Vector header
Cisco Unified Communications Manager 8.6(1) supports pass through of a SIP header called P-Charging-Vector (PCV) in network deployment. This PCV header is used to convey mobile or PSTN charging related information, such as the globally unique IP Multimedia Subsystem (IMS) charging identifier (ICID) value to the service providers.

A new SIP Normalization script, HCS-PCV-PAI-passthrough, is introduced as part of this feature. This script would be pre-installed on the Cisco Unified Communications Manager and has to be associated with all the SIP trunks that point to the network.
For any calls that originate from a network, the Cisco Unified Communications Manager passes through the PCV header received from a network in the INVITE, UPDATE and 200 OK to the other side. Cisco Unified Communications Manager would additionally pass through the PCV header from a network via 200 OK SIP for the calls terminating in the Cisco Unified Communications Manager. Because these calls are routed back to the Cisco network via the same SIP trunk, the 200 OK message received by the Cisco Unified Communications Manager is passed as-is through the PCV header in the outgoing calls.

**RFC3265 + Dialog Package**

This SIP standard supports the following Cisco Unified Communications Manager feature:

- Shared Line: Remote State Notifications

**RFC3265 + Presence Package**

These SIP standards support the following Cisco Unified Communications Manager features:

- BLF on Speed Dial
- BLF on Missed, Placed, Received Calls lists

**RFC3265 + KPML Package**

These SIP standards support the following Cisco Unified Communications Manager features:

- Digit Collection
- OOB DTMF

**RFC3265 + RFC3842 MWI Package (unsolicited notify)**

These SIP standards support the following Cisco Unified Communications Manager feature:

- Message Waiting Indication

**Remotecc**

This SIP standard supports the following Cisco Unified Communications Manager features:

- Ad hoc conferencing
- Remove Last Participant
- Conflist
- Immediate Diversion
- Call Park
- Call Select
- Shared Line: Privacy
**RFC4028 session timers**

This SIP standard allows periodic refresh of the SIP sessions through re-INVITE and allows Cisco Unified Communications Manager to determine whether the signalling connection to the remote is still active.

**Cisco Unified Communications Manager functionality that is supported by phones that are running SIP**

Cisco Unified Communications Manager supports the functions on Cisco Unified IP Phones described in this section.

**Dial plans**

Unlike the phones that are running SCCP, the phones that are running SIP collect digits locally before sending them to Cisco Unified Communications Manager. The phones that are running SIP use a local dial plan to know when enough digits have been entered and to trigger an INVITE with the collected digits. Phones that are running SIP that are in SRST mode will continue to use any configured dial plans that they receive from Cisco Unified Communications Manager. See SIP dial rules, on page 206, for more information.

**Do not disturb**

Cisco Unified Communications Manager supports do not disturb (DND) that a SIP device initiates or that a Cisco Unified Communications Manager device initiates. A DND status change gets signaled from a SIP device to Cisco Unified Communications Manager that is using the SIP PUBLISH method. A DND status change gets signaled from a Cisco Unified Communications Manager to a SIP device that is using a dndupdate Remote-cc REFER request. Cisco Unified Communications Manager can also publish the do not disturb status for a device, along with the busy and idle status for the device.

**PLAR**

Private Line Automatic Ringdown (PLAR), a term that is used by traditional telephony systems, refers to a phone configuration whereby any time the user goes off hook, the phone immediately dials a preconfigured number. The user cannot dial any other numbers from that phone (or line). This gets implemented in SCCP IP phones in Cisco Unified Communications Manager by using partitions, calling search space (CSS), and translation patterns; neither the device configuration nor line configuration indicates that PLAR is set up for the phone.

Administrators use SIP Dial Rules for configuring PLAR in phones that are running SIP. Phones that are configured for PLAR will have a one-line dial plan configuration that specifies the appropriate target pattern. When the user goes off hook, the phone will populate the INVITE with the target string and immediately send the request to Cisco Unified Communications Manager. The user does not enter any digits. See SIP dial rules, on page 206 for more information.

**Softkey handling**

The administrator uses Cisco Unified Communications Manager Administration to modify the softkey sets that the phone displays. You can add and remove keys, and their positions can get changed. This data gets
written to the database and gets sent to the phone that is running SCCP via Station messages as part of the phone registration/initialization process. For Cisco Unified IP Phones that support SIP, however, instead of sending the keys in Station Messages, the Cisco Unified Communications Manager TFTP server builds the file that contains the softkey sets. The phone that is running SIP retrieves these files from the TFTP server, and the new softkey sets overwrite the softkey sets that are built into the phone. This allows Cisco Unified Communications Manager to modify the default softkeys and also lets Cisco Unified Communications Manager manipulate the softkey events, so it can directly control some phone-level features.

For features that are configured by using the Softkey Configuration window but are not supported by the phone that is running SIP, the softkey will display, but the phone will display a message that the key is not active, which is consistent with the behavior of the phone that is running SCCP.

The Dial softkey appears as part of the default softkey set when the phone that is running SIP is operating in SRST mode.

---

Note

The Cisco Unified IP Phones 7905, 7912, 7940, and 7960 that are running SIP do not download softkeys. These phones get their softkey configuration in the phone firmware.

---

DSCP configuration

Cisco Unified IP Phones that are running SIP get their DSCP information from the configuration file that gets downloaded to the device. The DSCP setting applies for the device, whereas, the phones that are running SCCP can get the DSCP setting for a call. DSCP values get configured in the Enterprise Parameters Configuration window, and in the Cisco Unified Communications Manager Service Parameters Configuration window.

SIP profiles for endpoints

Because SIP attributes rarely change, Cisco Unified Communications Manager uses SIP profiles to define SIP attributes that are associated with SIP trunks and Cisco Unified IP Phones. Having these attributes in a profile instead of adding them individually to every SIP trunk and phone that is running SIP decreases the amount of time administrators spend configuring SIP devices and allows the administrator to change the values for a group of devices. Because the SIP profile is a required field when SIP trunks and phones are configured, Cisco Unified Communications Manager provides a default SIP profile; however, administrators can create customized SIP profiles. SIP profiles get assigned to SIP devices by using Cisco Unified Communications Manager Administration.

The software on the phone that is running SIP uses the majority of SIP values that are sent via TFTP to the phones.

For information on configuring SIP profiles, see SIP dial rules, on page 206.

Network Time Protocol (NTP)

You can configure phone Network Time Protocol (NTP) references in Cisco Unified Communications Manager Administration to ensure that a Cisco Unified IP Phone that is running SIP gets its date and time from the NTP server. If all NTP servers do not respond, the phone that is running SIP uses the date header in the 200 OK response to the REGISTER message for the date and time.
After you add the phone NTP reference to Cisco Unified Communications Manager Administration, you must add it to a date/time group. In the date/time group, you prioritize the phone NTP references, starting with the first server that you want the phone to contact.

The date/time group configuration gets specified in the device pool, and the device pool gets specified in the phone window.

For information on configuring the NTP reference, see SIP dial rules, on page 206.

**CTI support**

Line-side SIP includes CTI functionality, which allows CTI applications such as Cisco Unified Communications Manager Assistant to support Cisco Unified IP Phones that are running SIP (for example, Cisco Unified IP Phone 7961). CTI capabilities on phones that are running SIP equate to those on phones that are running SCCP with a few exceptions. Some CTI features that are supported on phones that are running SIP include display text, set lamp, play tone, call park, and privacy support. For more information about CTI and Cisco Unified Communications Manager, see Computer Telephony Integration, on page 577.

**Single button Barge/cBarge**

Cisco Unified Communications Manager supports Single Button Barge/cBarge that a SIP device initiates. The Single Button Barge/cBarge capabilities on phones that are running SIP equate to those on phones that are running SCCP. The Single Button Barge/cBarge feature allows a user to simply press the shared-line button of a call that is in progress, to automatically add that user to the call.

**Join and Join Across Lines**

The Join feature operates similar to one or more instances of the ad-hoc conference feature for phones that are running SIP, except for without the consultative call. The Join Across Lines feature allows a user to join calls on multiple phone lines (either on different directory numbers or on the same directory number but on different partitions) to create a conference.

When a user initiates the Join or Join Across Lines feature, the phone that is running SIP will use the Join softkey message in the same way existing softkeys are sent to Cisco Unified Communications Manager from phones that are running SIP to invoke the join feature on selected lines.

**Programmable line keys**

Cisco Unified IP Phones support line buttons (the buttons to the right of the display), which are used to initiate, answer, or switch to a call on a particular line. A limited number of features, such as speed dial, extension mobility, privacy, BLF speed dial, DND, and Service URLs, get assigned to these buttons. Each of these features are supported on phones that are running SIP and can be configured in Cisco Unified Communications Manager.

For information on the PLK feature, see Programmable line keys, on page 512.

**Malicious Call Identification (MCID)**

Cisco Unified Communications Manager supports the MCID feature on phones that are running SIP. The MCID capabilities on phones that are running SIP equate to those on phones that are running SCCP. The MCID feature provides a useful method for tracking troublesome or threatening calls. When a user receives
this type of call and presses the MCID softkey, a new Remote-cc REFER softkey event request is sent to Cisco Unified Communications Manager. This triggers Cisco Unified Communications Manager to record the call. The user is then sent a confirmation tone and a text message to acknowledge receiving the MCID notification. The confirmation tone is handled by a Remote-cc playtonereq to the phone, and the text message is a Remote-cc statuslineupdate indicating “Mcid Successful”.

**Single call UI**

Cisco Unified Communications Manager supports a single call UI with the use of line rollovers on phones that are running SIP. A line rollover occurs if the max-calls-per-line and busy-trigger values are set to 1/1. For Transfer and Conference features, when the max-calls-per-line value is reached on the primary call, the phone can roll over the consult call to the closest line button with zero calls, or on the same DN in a different partition. If the max-calls-per-line and busy-trigger values are set to 2/1, the outbound consult call will be carried on the same button.

**Directed Call Pickup**

Cisco Unified Communications Manager supports the Directed Call Pickup feature on phones that are running SIP. The Directed Call Pickup capabilities on phones that are running SIP equate to those on phones that are running SCCP. Directed Call Pickup allows you to pick up an alerting call on a DN directly by pressing the GPickUp softkey and entering the directory number. The phone that is running SIP will then send Cisco Unified Communications Manager an INVITE that includes the DN of the phone that you want to pick up.

**Unified Mobile Communications Server (UMCS) integration**

Cisco Unified Communications Manager supports integration with UMCS to extend the capabilities of Cisco Unified Communications Manager to Cisco Unified Mobile Communicator devices. The UMCS communicates with Cisco Unified Communications Manager using SIP over one or more TCP connections. Each TCP connection can be shared between multiple users.

**Do Not Disturb (DND) Call Reject**

The DND feature allows you to set one of two options in Cisco Unified CM User Options. You can set the DND feature to Ringer Off or Call Reject. Call Reject gets supported on both phones that are running SCCP and phones that are running SIP. When DND is active and Call Reject is selected, no incoming calls or audio and visual notifications get presented on the phone.

**BLF Call Pickup**

Cisco Unified Communications Manager allows you to assign a line key as a BLF Call Pickup key. The BLF Call Pickup key behaves the same way as a BLF speed dial key on phones that are running SIP. The line key indicates the BLF status of the configured DN, and pressing the line key speed dials the configured DN. BLF Call Pickup adds an alerting indication when a call is alerting on the DN configured as the BLF Call Pickup DN. You can answer the alerting call by pressing the BLF Call Pickup DN while the call is showing an alerting state.

The subscription type PRESENCE+ALERTING is used by the SIP device layer to subscribe for the presence and alerting status of calls on a DN monitored by the BLF Call Pickup feature. The subscription for
PRESENCE+ALTERTING is handled by the line control of the monitored DN line. Line Control is responsible for notifying the Subscription Manager when a call is received for a DN that has been subscribed for.

Calling party normalization

Cisco Unified Communications Manager allows you to globalize calling party numbers of calls received through gateways. The calling party number can be transformed into E.164 format before being presented on the phone. This globalized number gets provided to the phone, so a user can dial back a received number without having to use the edit dial function.

An optional URI parameter (x-cisco-callback-number) for globalized numbers is added to the RPID header. The localized number is specified as the user part of the SIP URI. The same SIP URI is also specified in the From header sent by the Cisco Unified Communications Manager to the phone. When invoking the dial back feature, the phone will echo back the same SIP URI as the request URI in the INVITE to Cisco Unified Communications Manager. The Cisco Unified Communications Manager SIP Device layer will parse the request URI for the URI parameter containing the globalized number to use for routing. If it is not found, the SIP device layer will resort to using the localized form of the number found in the user portion of the SIP URI.

Be aware that the x-cisco-callback-number parameter is optional and will not get included in the RPID header of a conference call, and it will not get included when a call is marked as private.

E.164

Cisco Unified Communications Manager allows you to globalize calling party numbers of calls received through gateways. This includes the addition of the “+” sign found in E.164 formatted numbers, such as +14085551234. When a phone that is running SIP invokes the dial back feature from the call logs directory, the globalized number will get returned to the Cisco Unified Communications Manager for routing. E.164 support allows the SIP device layer to pass the entire globalized number string, including the + sign, to the DA.

Soft client dual registration

Cisco Unified Communications Manager does not allow two different endpoints to register to the same device name. For soft clients, this can present a problem because a soft client can be installed on multiple systems, such as a Cisco Jabber client for PC and a Cisco Jabber client for Macintosh, and can use the same registration from each system.

To handle registration attempts where a different soft client is already registered to that device name, soft clients can insert the following tags into the Supported header of SIP registration requests:

- **x-cisco-duplicate-reg**—When this tag is present, Cisco Unified Communications Manager automatically registers the second soft client and drops the first soft client registration.

- **x-cisco-graceful-reg**—This tag was introduced for release 9.0. The tag gives a soft client that is attempting to register to a registered device name the ability to gracefully override the existing registration session without having to automatically cancel the existing session. When this tag is present, Cisco Unified Communications Manager rejects the new registration attempt and returns a SIP 403 message. The soft client can either send a new registration attempt using just the x-cisco-duplicate-reg tag, which would de-register the first soft client, or abort the registration attempt, which would keep the first soft client registration intact.
If both tags are present, Cisco Unified Communications Manager gives precedence to the \textit{x-graceful-reg} tag.
This chapter provides information about trunk types. In a distributed call-processing environment, Cisco Unified Communications Manager communicates with other Cisco Unified Communications Manager clusters, the public switched telephone network (PSTN), and other non-IP telecommunications devices, such as private branch exchanges (PBXs) by using trunk signaling protocols and voice gateways.

- Set up SIP trunk, page 449
- Cisco Unified Communications Manager trunk configuration, page 451
- Trunks and the Calling Party Normalization feature, page 454
- Apply the international escape character to inbound calls over H.323 trunks, page 455
- Transfer calls between trunks, page 456
- Dependency records for trunks and associated route groups, page 458
- H.235 support for trunks, page 458

### Set up SIP trunk

For SIP Trunks follow these steps:

**Procedure**

**Step 1** Gather the endpoint information, such as IP addresses or host names, that you need to configure the trunk interface.

Cisco Unified Communications Solution Reference Network Design (SRND)
Set up SIP trunk

Step 2  Configure the SIP proxy.
Step 3  Create a SIP profile.
Step 4  Create a SIP trunk security profile.
Step 5  Create a SIP trunk. For trunk security, check the SRTP Allowed check box and then choose the Consider Traffic on This Trunk Secure settings (optional).
Step 6  Configure the destination address.
Step 7  Configure the destination port.
Step 8  Associate the SIP trunk to a Route Pattern or Route Group.
Step 9  Reset the SIP trunk.
Step 10 Configure SIP timers, counters, and service parameters, if necessary. If you are using PUBLISH to communicate to a Cisco Unified Presence, choose the configured trunk in the CUP PUBLISH Trunk field of the Service Parameters Configuration window.

Tip  Verify that the The SIP Interoperability Enabled service parameter, which supports the Cisco CallManager service, is set to True; when you set this parameter to False, Cisco Unified Communications Manager ignores SIP messages, and SIP devices do not function; that is, phones that run SIP cannot register with Cisco Unified Communications Manager and SIP trunks cannot interact with Cisco Unified Communications Manager. The default value specifies True. You must restart the Cisco CallManager service if you change the value of this parameter.

Step 11 To facilitate interoperability among a variety of endpoints, including PBXs, gateways, and service providers, you may need to enable SIP normalization and transparency. Normalization allows you to preserve, remove, or change the contents of any SIP headers or content bodies, known or unknown. To enable normalization, you create scripts as described in the Developer Guide for SIP Transparency and Normalization and import them in Cisco Unified Communications Manager Administration. SIP transparency allows you to pass information from one call leg to the other. You enable SIP transparency using scripting, as described in the Developer Guide for SIP Transparency and Normalization. You can also enable REFER transparency so that Cisco Unified Communications Manager passes on REFER requests to another endpoint rather than acting on them. To do so, apply the precanned REFER transparency script (refer-passthrough.lua) or a custom script imported from the SIP Normalization Script Configuration window (Device > Device Settings > SIP Normalization Script) to the SIP trunk by configuring the Normalization Script fields on the Trunk Configuration window (Device > Trunk).

Step 12 To configure an early offer enabled SIP trunk, edit the SIP profile, and check the Early Offer support for voice and video calls (insert MTP if needed) check box.

Note  Make sure that the MTP uses IOS version 15.1(2)T or later.

Step 13 If you use SCCP phones with SCCP version 20 support (which provides media port information through the getPort capability) and you enabled early offer on a SIP trunk, set the following CallManager service parameters (System > Service Parameters):

• Port Received Timer for Outbound Call Setup
• Port Received Timer After Call Connection
• Fail Call Over SIP Trunk if MTP Allocation Fails
• Fail Call If Trusted Relay Point Allocation Fails

Step 14 To prevent Cisco Unified Communications Manager from sending an INVITE a=inactive SDP message during call hold or media break during supplementary services, edit the appropriate SIP profile, and check the Send send-receive SDP in mid-call INVITE check box. When you enable Send send-receive SDP in mid-call INVITE for an early offer SIP trunk in tandem mode, Cisco Unified Communications Manager inserts MTP
to provide sendrecv SDP when a SIP device sends offer SDP with a=inactive or sendonly or recvonly in audio media line. In tandem mode, Cisco Unified Communications Manager depends on the SIP devices to initiate reestablishment of media path by sending either a delayed offer INVITE or mid-call INVITE with send-receive SDP. When you enable both **Send send-receive SDP in mid-call INVITE** and **Require SDP Inactive Exchange for Mid-Call Media Change** on the same SIP profile, the Send send-receive SDP in mid-call INVITE setting overrides the Require SDP Inactive Exchange for Mid-Call Media Change setting, so Cisco Unified Communications Manager does not send an INVITE with a=inactive SDP in mid-call codec updates. For SIP line side calls, the Require SDP Inactive Exchange for Mid-Call Media Change check box applies when enabled.

**Note** This check box applies only to early offer enabled SIP trunks and has no impact on SIP line calls.

**Note** To prevent the SDP mode from being set to inactive in a multiple-hold scenario, set the Duplex Streaming Enabled clusterwide service parameter (**System > Service Parameters**) to **True**.

**Step 15** To track the status of remote destinations, configure SIP OPTIONS. Use SIP Profile Configuration to enable SIP OPTIONS. Check the **Enable OPTIONS Ping to monitor destination status for trunks with service type “None (Default)”** check box.

---

**Cisco Unified Communications Manager trunk configuration**

Trunk configuration in Cisco Unified Communications Manager Administration depends on the network design and call-control protocols that are used in the IP WAN. All protocols require that either a signaling interface (trunk) or a gateway be created to accept and originate calls. For some IP protocols, such as MGCP, you configure trunk signaling on the gateway. You specify the type of signaling interface when you configure the gateway in Cisco Unified Communications Manager. For example, to configure QSIG connections to Cisco Unified Communications Manager, you must add an MGCP voice gateway that supports QSIG protocol to the network. You then configure the T1 PRI or E1 PRI trunk interface to use the QSIG protocol type. For more information about configuring gateways, see the *Cisco Unified Communications Manager voice gateways overview*, on page 357.

**Related Topics**

- Trunks and gatekeepers in Cisco Unified Communications Manager, on page 451
- Trunk types in Cisco Unified Communications Manager administration, on page 452

**Trunks and gatekeepers in Cisco Unified Communications Manager**

In addition to using gateways to route calls, you can configure trunks in Cisco Unified Communications Manager Administration to function as described in the sections which follow.

**Related Topics**

- Cisco Unified Communications Manager trunk configuration, on page 451

**Gatekeeper-controlled trunks**

Gatekeepers that are used in a distributed call-processing environment provide call routing and call admission control for Cisco Unified Communications Manager clusters. Intercluster trunks that are gatekeeper-controlled can communicate with all remote clusters. Similarly, an H.225 trunk can communicate with any H.323
gatekeeper-controlled endpoints including Cisco Unified Communications Manager clusters. Route patterns or route groups can route the calls to and from the gatekeeper. In a distributed call-processing environment, the gatekeeper uses the E.164 address (phone number) and determines the appropriate IP address for the destination of each call, and the local Cisco Unified Communications Manager uses that IP address to complete the call.

For large distributed networks where many Cisco Unified Communications Manager clusters exist, you can avoid configuring individual intercluster trunks between each cluster by using gatekeepers.

When you configure gatekeeper-controlled trunks, Cisco Unified Communications Manager creates a virtual trunk device. The gatekeeper changes the IP address of this device dynamically to reflect the IP address of the remote device. Specify these trunks in the route patterns or route groups that route calls to and from the gatekeeper.

See *Cisco Unified Communications Solution Reference Network Design (SRND)* for more detailed information about gatekeeper configuration, dial plan considerations when using a gatekeeper, and gatekeeper interaction with Cisco Unified Communications Manager.

**Non-gatekeeper-controlled trunks**

With no gatekeepers in the distributed call-processing environment, you must configure a separate intercluster trunk for each remote device pool in a remote cluster that the local Cisco Unified Communications Manager can call over the IP WAN. You also configure the necessary route patterns and route groups to route calls to and from the various intercluster trunks. The intercluster trunks statically specify the IP addresses of the remote devices.

**Related Topics**

- Trunk types in Cisco Unified Communications Manager administration, on page 452

**Trunk types in Cisco Unified Communications Manager administration**

Your choices for configuring trunks in Cisco Unified Communications Manager depend on whether the IP WAN uses gatekeepers to handle call routing. Also, the types of call-control protocols that are used in the call-processing environment determine trunk configuration options.

You can configure the trunk types in Cisco Unified Communications Manager Administration listed in this section.

**Related Topics**

- Non-gatekeeper-controlled trunks, on page 452
- Cisco Unified Communications Manager trunk configuration, on page 451

**H.225 trunk (gatekeeper controlled)**

In an H.323 network that uses gatekeepers, use an H.225 trunk with gatekeeper control to configure a connection to a gatekeeper for access to other Cisco Unified Communications Manager clusters and to H.323 devices. An H.225 trunk can communicate with any H.323 gatekeeper-controlled endpoint. When you configure an H.323 gateway with gatekeeper control in Cisco Unified Communications Manager Administration, use an H.225 trunk. To choose this method, use Device > Trunk and choose H.225 Trunk (Gatekeeper Controlled).

You also configure route patterns and route groups to route calls to and from the gatekeeper. For more information, see the Configure gatekeepers and trunks, on page 74.
Intercluster trunk (gatekeeper controlled)

In a distributed call-processing network with gatekeepers, use an intercluster trunk with gatekeeper control to configure connections between clusters of Cisco Unified Communications Manager systems. Gatekeepers provide call admission control and address resolution for intercluster calls. A single intercluster trunk can communicate with all remote clusters. To choose this method, use Device > Trunk and choose Inter-Cluster Trunk (Gatekeeper Controlled) in Cisco Unified Communications Manager Administration.

You also configure route patterns and route groups to route the calls to and from the gatekeeper. In this configuration, the gatekeeper dynamically determines the appropriate IP address for the destination of each call, and the local Cisco Unified Communications Manager uses that IP address to complete the call.

For more information about gatekeepers, see the Configure gatekeepers and trunks, on page 74.

Intercluster trunks support location-based call admission control (CAC) through use of the specially designated Phantom location. See Location-based call admission control over intercluster trunk, on page 73 for additional information.

Intercluster trunk (non-gatekeeper controlled)

In a distributed network that has no gatekeeper control, you must configure a separate intercluster trunk for each device pool in a remote cluster that the local Cisco Unified Communications Manager can call over the IP WAN. The intercluster trunks statically specify the IP addresses or host names of the remote devices. To choose this method, use Device > Trunk and choose Inter-Cluster Trunk (Non-Gatekeeper Controlled) in Cisco Unified Communications Manager Administration.

You must specify the IP addresses of all remote Cisco Unified Communications Manager nodes that belong to the device pool of the remote non-gatekeeper-controlled intercluster trunk.

You also configure the necessary route patterns and route groups to route calls to and from the intercluster trunks.

Intercluster trunks support location-based call admission control (CAC) through use of the specially designated Phantom location. See Location-based call admission control over intercluster trunk, on page 73 for additional information.

SIP trunk

In a call-processing environment that uses Session Initiation Protocol (SIP), use SIP trunks to configure a signaling interface with Cisco Unified Communications Manager for SIP calls. SIP trunks (or signaling interfaces) connect Cisco Unified Communications Manager clusters with a SIP proxy server. The SIP signaling interface uses requests and responses to establish, maintain, and terminate calls (or sessions) between two or more endpoints.

To configure a SIP trunk in Cisco Unified Communications Manager Administration, choose Device > Trunk and then SIP Trunk.

You must also configure route groups and route patterns that use the SIP trunks to route the SIP calls.
To receive QSIG basic calls and features, such as MWI, Call Transfer, Call Diversion, Call Completion, Path Replacement, and Identification Services, across an intercluster SIP trunk or a SIP gateway, configure a SIP trunk with QSIG as the tunneled protocol.

**Note**

Remote-Party-ID (RPID) headers coming in from the SIP gateway can interfere with QSIG content and cause unexpected behavior with Call Back capabilities. To prevent interference with the QSIG content, turn off the RPID headers on the SIP gateway.

To turn off RPID headers on the SIP gateway, apply a SIP profile to the VoIP dial peer on the gateway, as shown in the following example:

```
voice class sip-profiles 1000
request ANY sip-header Remote-Party_ID remove
response ANY sip-header Remote-Party-ID remove
dial-peer voice 124 voip
destination-pattern 3...
signaling forward unconditional
session protocol sipv2
session target ipv4:<ip address>
voice-class sip profiles 1000
```

SIP trunks support location-based call admission control (CAC) through use of the specially designated Phantom location.

**Note**

When you create a SIP trunk with Cisco Intercompany Media Engine (IME) selected as the trunk service type, the default for the Tunneled Protocol field is QSIG. QSIG must be the tunneled protocol for QSIG features to work on a Cisco IME trunk. For more information about Cisco IME, see the Cisco Intercompany Media Engine Installation and Configuration Guide.

**Related Topics**

- Location-based call admission control over intercluster trunk, on page 73
- SIP and Cisco Unified Communications Manager, on page 398
- Cisco Unified Communications Manager SIP endpoints overview, on page 438
- Block transfer capabilities by using service parameters, on page 457
- Dependency records for trunks and associated route groups, on page 458

**Trunks and the Calling Party Normalization feature**

In line with E.164 standards, calling party normalization enhances the dialing capabilities of some phones and improves call back functionality when a call is routed to multiple geographical locations; that is, the feature ensures that the called party can return a call without needing to modify the directory number in the call log directories on the phone. Additionally, calling party normalization allows you to globalize and localize phone numbers, so the appropriate calling number presentation displays on the phone.
Configuring calling party normalization alleviates issues with toll bypass where the call is routed to multiple locations over the IP WAN. In addition, it allows Cisco Unified Communications Manager to distinguish the origin of the call to globalize or localize the calling party number for the phone user.

SIP trunks and MGCP gateways can support sending the international escape character, +, for calls. H.323 gateways/trunks do not support the + because the H.323 protocol does not support the international escape character, +. QSIG trunks do not attempt to send the +. For outgoing calls through a gateway that supports +, Cisco Unified Communications Manager can send the + with the dialed digits to the gateway/trunk. For outgoing calls through a gateway/trunk that does not support +, the international escape character + gets stripped when Cisco Unified Communications Manager sends the call information to the gateway/trunk.

SIP does not support the number type, so calls through SIP trunks only support the Incoming Calling Party Unknown Number (prefix and digits-to-strip) settings.

You can configure the international escape character, +, to globalize the calling party number. For information on the international escape character, +, see Use the international escape character, on page 161.

### Apply the international escape character to inbound calls over H.323 trunks

The H.323 protocol does not support the international escape character, +. To ensure that correct prefixes, including the international escape character, +, get applied for inbound calls over H.323 gateways/trunks, you must configure the incoming called party settings in the service parameter, device pool, H.323 gateway, or H.323 trunk windows; that is, configuring the incoming called party settings ensures that when an inbound call comes from a H.323 gateway or trunk, Cisco Unified Communications Manager transforms the called party number back to the value that was originally sent over the trunk/gateway.

For example, to ensure that the correct DN patterns get used with SAF/call control discovery for inbound calls over H.323 gateways/trunks, you must configure the incoming called party settings in the service parameter, device pool, or H.323 (non-gatekeeper controlled) trunk window. See the following example for more information.

- A caller places a call to +19721230000 to Cisco Unified Communications Manager A.
- Cisco Unified Communications Manager A receives +19721230000 and transforms the number to 55519721230000 before sending the call to the H.323 trunk. In this case, your configuration indicates that the international escape character + should be stripped and 555 should be prepended for calls of International type.
- For this inbound call from the trunk, Cisco Unified Communications Manager B receives 55519721230000 and transforms the number back to +19721230000 so that digit analysis can use the value as it was sent by the caller. In this case, your configuration for the incoming called party settings indicates that you want 555 to be stripped and +1 to be prepended to called party numbers of International type.

You can configure the incoming called party settings in the service parameter, device pool, H.323 gateway, or H.323 (gatekeeper-controlled) windows.

The service parameters support the Cisco CallManager service. To configure the service parameters, click Advanced in the Service Parameter Configuration window for the Cisco CallManager service; then, locate the H.323 pane for the following parameters:

- Incoming Called Party National Number Prefix - H.323
- Incoming Called Party International Number Prefix - H.323
- Incoming Called Party Subscriber Number Prefix - H.323
Incoming Called Party Unknown Number Prefix - H.323

These service parameters allow you to prefix digits to the called number based on the Type of Number field for the inbound offered call. You can also strip a specific number of leading digits before the prefix gets applied. To prefix and strip digits by configuring these parameter fields, use the following formula, x:y, where x represents the exact prefix that you want to add to called number and y represents the number of digits stripped; be aware that the colon separates the prefix and the number of stripped digits. For example, enter 91010:6 in the field, which means that you want to strip 6 digits and then add 901010 to the beginning of the called number. In this example, a national call of 2145551234 becomes 910101234. You can strip up to 24 digits and prefix/add up to 16 digits.

Transfer calls between trunks

Using Cisco Unified Communications Manager Administration, you can configure trunks as OnNet (internal) trunks or OffNet (external) trunks by using Trunk Configuration or by setting a clusterwide service parameter. Used in conjunction with the clusterwide service parameter, Block OffNet to OffNet Transfer, the configuration determines whether calls can be transferred over a trunk.

To use the same trunk to route both OnNet and OffNet calls, associate the trunk with two different route patterns. Make one trunk OnNet and the other OffNet with both having the Allow Device Override check box unchecked.

Transfer capabilities using trunk configuration

Using Cisco Unified Communications Manager Administration Trunk Configuration, you can configure a trunk as OffNet or OnNet. The system considers calls that are coming to the network through that trunk as OffNet or OnNet, respectively. Use the Trunk Configuration window field, Call Classification, to configure the trunk as OffNet, OnNet, or Use System Default. See the following table for a description of these settings.

The Route Pattern Configuration window provides a drop-down list box called Call Classification, which allows you to configure a route pattern as OffNet or OnNet. When Call Classification is set to OffNet and the Allow Device Override check box is unchecked, the system considers the outgoing calls that use this route pattern as OffNet (if configured as OnNet and check box is unchecked, outgoing calls are considered OnNet).

You can use the same trunk to route both OnNet and OffNet calls by associating the trunk with two different route patterns: one OnNet and the other OffNet, with both having the Allow Device Override check box unchecked. For outgoing calls, the outgoing device setting classifies the call as either OnNet or OffNet by determining whether the Allow Device Override check box is checked.

In route pattern configuration, if the Call Classification is set as OnNet, the Allow Device Override check box is checked, and the route pattern is associated with an OffNet Trunk, the system considers the outgoing call as OffNet.

Table 40: Trunk Configuration Call Classification Settings

<table>
<thead>
<tr>
<th>Setting Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OffNet</td>
<td>This setting identifies the trunk as being an external trunk. When a call comes in from a trunk that is configured as OffNet, the outside ring gets sent to the destination device.</td>
</tr>
</tbody>
</table>
### Setting Name | Description
---|---
OnNet | This setting identifies the trunk as being an internal trunk. When a call comes in from a trunk that is configured as OnNet, the inside ring gets sent to the destination device.
Use System Default | This setting uses the Cisco Unified Communications Manager clusterwide service parameter Call Classification.

---

### Set up transfer capabilities by using Call Classification service parameter

To configure all trunks to be OffNet (external) or OnNet (internal), perform the following two steps:

**Procedure**

| Step 1 | Use the Cisco Unified Communications Manager clusterwide service parameter Call Classification. |
| Step 2 | Configure individual trunks to Use System Default in the Call Classification field that is on the Trunk Configuration window. |

---

### Block transfer capabilities by using service parameters

Block transfer restricts the transfer between external devices, so fraudulent activity gets prevented. You can configure the following devices as OnNet (internal) or OffNet (external) to Cisco Unified Communications Manager:

- H.323 gateway
- MGCP FXO trunk
- MGCP T1/E1 trunk
- Intercluster trunk
- SIP trunk

If you do not want OffNet calls to be transferred to an external device (one that is configured as OffNet), set the Cisco Unified Communications Manager clusterwide service parameter, Block OffNet to OffNet Transfer, to True.

If a user tries to transfer a call on an OffNet trunk that is configured as blocked, a message displays on the user phone to indicate that the call cannot be transferred.

**Related Topics**

SIP trunk, on page 453
Dependency records for trunks and associated route groups

To find route groups that use a specific trunk, choose Dependency Records from the Related Links drop-down list box that is provided on the Cisco Unified Communications Manager Administration Trunk Configuration window. The Dependency Records Summary window displays information about route groups that are using the trunk. To find more information about the route group, click the route group, and the Dependency Records Details window displays. If the dependency records are not enabled for the system, the dependency records summary window displays a message.

**Related Topics**

- SIP trunk, on page 453

H.235 support for trunks

This feature allows Cisco Unified Communications Manager trunks to transparently pass through the shared secret (Diffie-Hellman key) and other H.235 data between two H.235 endpoints so that the two endpoints can establish a secure media channel.
This chapter provides information about Cisco Unified IP Phones which, as full-featured telephones, can plug directly into your IP network. H.323 clients, CTI ports, and Cisco IP Communicator represent software-based devices that you configure similarly to the Cisco Unified IP Phones. Cisco Unified Communications Manager Administration allows you to configure phone features such as call forwarding and call waiting for your phone devices. You can also create phone button templates to assign a common button configuration to a large number of phones.

After you have added the phones, you can associate users with them. By associating a user with a phone, you give that user control over that device.

- Phone configuration, page 460
- Supported Cisco Unified IP phones, page 462
- Third-party SIP endpoints, page 479
- H.323 clients and CTI ports, page 479
- CTI remote device setup, page 480
- Client Services Framework setup, page 484
- Cisco IP Communicator, page 500
- Cisco Unified Personal Communicator, page 500
- Cisco TelePresence, page 501
- Cisco Unified Mobile Communicator, page 501
- Codec usage, page 501
- Phone button templates, page 503
- Programmable line keys, page 512
- Softkey templates, page 514
- Softkey template operation, page 517
- Common phone profiles, page 518
- Methods for adding phones, page 518
- Phone migration, page 519
Phone configuration

Cisco Unified IP Phones, as full-featured telephones, can plug directly into your IP network. H.323 clients, CTI ports, and Cisco IP Communicator represent software-based devices that you configure similarly to the Cisco Unified IP Phones. Cisco Unified Communications Manager Administration allows you to configure phone features such as call forwarding and call waiting for your phone devices. You can also create phone button templates to assign a common button configuration to a large number of phones.

After you have added the phones, you can associate users with them. By associating a user with a phone, you give that user control over that device.

The following sections provides steps to manually configure phone that runs SCCP, and to manually configure a phone that runs SIP in Cisco Unified Communications Manager Administration. If you are using autoregistration, Cisco Unified Communications Manager adds the phone and automatically assigns the directory number.

Configure phone for SCCP

Procedure

Step 1 Gather the following information about the phone:

- Model
- MAC address
- Physical location of the phone
- Cisco Unified Communications Manager user to associate with the phone
- Partition, calling search space, and location information, if used
- Number of lines and associated DNs to assign to the phone

Phone search, on page 538
Step 2  Add and configure the phone.
Step 3  If security is required, configure the phone security profile. The phone security profile gets added to the phone by choosing a phone security profile in the Phone Configuration window.
Step 4  If the phone will be used outside of the trusted network, configure VPN client. The VPN connection is used for situations in which a phone is located outside a trusted network or when network traffic between the phone and Cisco Unified Communications Manager must cross untrusted networks.
Step 5  Add and configure lines (DNs) on the phone. You can also configure phone features such as call park, call forward, and call pickup.
Step 6  Configure speed-dial buttons. You can configure speed-dial buttons for phones if you want to provide speed-dial buttons for users or if you are configuring phones that do not have a specific user who is assigned to them. Users can change the speed-dial settings on their phones by using Cisco Unified CM User Options.
Step 7  Configure Cisco Unified IP Phone services. You can configure services for Cisco Unified IP Phones and Cisco IP Communicator if you want to provide services for users or if you are configuring phones that do not have a specific user who is assigned to them. Users can change the services on their phones by using Cisco Unified CM User Options.
Step 8  Customize phone button templates and softkey templates, if required. Configure templates for each phone.
Step 9  Configure the Busy Lamp Field feature, if required. You must use customized phone button templates to configure BLF/SpeedDial buttons.
Step 10  Assign services to phone buttons, if required.
Step 11  Provide power, install, verify network connectivity, and configure network settings for the Cisco Unified IP Phone.
Step 12  Associate user with the phone (if required).
Step 13  Make calls with the Cisco Unified IP Phone.

Configure phone for SIP
The configuration steps for Cisco Unified IP Phones that support SIP are as follows.

Procedure

Step 1  Gather the following information about the phone:

- Model
- MAC address
- Physical location of the phone
- Cisco Unified Communications Manager user to associate with the phone
- Partition, calling search space, and location information, if used
- Number of lines and associated DNs to assign to the phone

Phone search, on page 538
Step 2  If configuring a phone that runs SIP in a secure mode, configure the SIP Phone Port in the Cisco Unified CM Configuration window.

Step 3  If security is required, configure the phone security profile. The phone security profile gets added to the phone that runs SIP by choosing a phone security profile in the Phone Configuration window.

Step 4  If the phone will be used outside of the trusted network, configure VPN client. The VPN connection is used for situations in which a phone is located outside a trusted network or when network traffic between the phone and Cisco Unified Communications Manager must cross untrusted networks.

Step 5  Configure the SIP Profile. The SIP Profile gets added to the phone that runs SIP by choosing the profile in the Phone Configuration window.

Step 6  If you are using NTP for the timing synchronization, configure the NTP server by using the Phone NTP Reference Configuration window. Add the NTP server to Date/Time Group Configuration and then assign the date/time group to the device pool. Add the device pool to the phone that runs SIP by choosing the device pool in the Phone Configuration window.

Step 7  If you want the digits to be collected before sending them to Cisco Unified Communications Manager, configure a dial plan for the phone that runs SIP. Add the SIP Dial Rule to the phone that runs SIP by using the Phone Configuration window.

Step 8  Add and configure the phone that runs SIP.

Step 9  Add and configure lines (DNs) on the phone. You can also configure phone features such as call park, call forward, and call pickup.

Step 10  Configure speed-dial buttons. You can configure speed-dial buttons for phones if you want to provide speed-dial buttons for users or if you are configuring phones that do not have a specific user who is assigned to them. Users can change the speed-dial settings on their phones by using Cisco Unified CM User Options.

Step 11  Configure Cisco Unified IP Phone services. You can configure services for Cisco Unified IP Phones and Cisco IP Communicator if you want to provide services for users or if you are configuring phones that do not have a specific user who is assigned to them. Users can change the services on their phones by using the Cisco Unified CM User Options window.

Step 12  Customize phone button templates and softkey templates, if required. Configure templates for each phone.

Step 13  Configure the Busy Lamp Field feature, if required. You must use customized phone button templates to configure BLF/SpeedDial buttons.

Step 14  Assign services to phone buttons, if required.

Step 15  Provide power, install, verify network connectivity, and configure network settings for the Cisco Unified IP Phone.

Step 16  Associate user with the phone (if required).

Step 17  Make calls with the Cisco Unified IP Phone.

---

**Supported Cisco Unified IP phones**

Table 36-3 provides an overview of the features that are available on the following Cisco Unified IP Phones that Cisco Unified Communications Manager supports:

- Cisco Unified IP Phone 6900 Series
- Cisco Unified IP Phone 7900 Series
- Cisco Unified IP Phone 8900 Series (SIP)
• Cisco Unified IP Phone 9900 Series (SIP)
• Cisco Unified IP Video Phone 7985 (SCCP)
• Cisco Unified IP Phone Expansion Module 7915 and 7916
• Cisco Unified IP Color Key Expansion Module
• Cisco IP Conference Station 7935, 7936, and 7937 (SCCP)
• Cisco Unified Wireless IP Phone 7921 and 7925 (SCCP)
• Cisco E20

For the latest information on features and services that these phone models support, see the following documentation:

• Phone administration or user documentation that supports the phone model and this version of Cisco Unified Communications Manager
• Firmware release notes for your phone model
• Cisco Unified Communications Manager release notes
Table 41: Supported Cisco Unified IP Phones and Features

<table>
<thead>
<tr>
<th>Cisco Unified IP Phone Model</th>
<th>Description</th>
</tr>
</thead>
</table>
| Cisco Unified IP Phone 9971 and 9951 | The Cisco Unified IP Phone 9971 and 9951 are advanced collaborative media endpoints that provide voice, video, applications, and accessories. Highlights include interactive multiparty video, high-resolution color touchscreen display, High-definition voice (HD voice), desktop Wi-Fi connectivity, Gigabit Ethernet and a new ergonomic design and user interface designed for simplicity and high usability. Accessories, which are sold separately, include the Cisco Unified Video Camera and the Cisco Unified IP Color Key Expansion Module. The Cisco Unified IP Phone 9971 supports the following buttons:  
  • Six feature buttons with state-indicating LEDs  
  • Six call-session buttons with state-indicating LEDs  
  • Applications, Directories, and Voicemail  
  • Conference, Transfer, and Hold  
  • Volume Up or Down  
  • Back-lit Mute, speakerphone, and headset  
  • Back, End Call, and 5-way navigation pad  
The Cisco Unified IP Phone 9951 supports the following buttons:  
  • Five feature buttons with state-indicating LEDs  
  • Five call-session buttons with state-indicating LEDs  
  • Applications, Directories, and Voicemail  
  • Conference, Transfer, and Hold  
  • Volume Up or Down  
  • Back-lit Mute, speakerphone, and headset  
  • Back, End Call, and 5-way navigation pad  
Both endpoints support Session Initiation Protocol (SIP). |
The Cisco Unified IP Phone 8961 (SIP) is an advanced professional media endpoint that delivers an enhanced user experience with an easy-to-use and eco-friendly ergonomic design. Highlights of the portfolio include introduction of higher-resolution (VGA) color displays, a USB port, Gigabit Ethernet connectivity, and High-definition (HD) voice support, enabling a more productive user experience for multimedia application engagement. Application support includes XML and MIDlet-enabled applications. The Cisco Unified IP Phone 8961 is an ideal solution for knowledge professionals, administrative managers, and executives.

The Cisco Unified IP Phone 8961 supports the following buttons:

- Five programmable feature buttons with state-indicating LEDs
- Five call-session buttons with state-indicating LEDs
- Applications, Directories, and Voicemail
- Conference, Transfer, and Hold
- Volume Up/Down,
- Back-lit Mute, Speakerphone, and Headset
- Back, End Call, and 5-Way Navigation Pad

Cisco Unified IP Phone 8961 supports Session Initiation Protocol (SIP).

The Cisco Unified IP Phone 7975 demonstrates the latest advances in VoIP telephony, including wideband audio support, backlit color touchscreen display, and an integrated Gigabit Ethernet port.

- This IP phone includes a large, backlit, easy-to-read color display for easy access to communication information, timesaving applications, and features such as date and time, calling party name, calling party number, digits dialed, and presence information.
- The phone provides direct access to eight telephone lines (or combination of lines, speed dials, and direct access to telephony features), five interactive softkeys that guide you through call features and functions, and an intuitive four-way (plus Select key) navigation cluster.
- A hands-free speakerphone and handset designed for high-fidelity wideband audio are standard, as is a built-in headset connection.

Cisco Unified IP Phone 7975 supports SCCP and SIP protocols.
<table>
<thead>
<tr>
<th>Cisco Unified IP Phone Model</th>
<th>Description</th>
</tr>
</thead>
</table>
| Cisco Unified IP Phone 7965  | The Cisco Unified IP Phone 7965 demonstrates the latest advances in VoIP telephony, including wideband audio support, backlit color display, and an integrated Gigabit Ethernet port.  
  - This IP phone includes a large, backlit, easy-to-read color display for easy access to communication information, timesaving applications, and features such as date and time, calling party name, calling party number, digits dialed, and presence information.  
  - The phone provides direct access to six telephone lines (or combination of lines, speed dials, and direct access to telephony features), four interactive softkeys that guide you through call features and functions, and an intuitive four-way (plus Select key) navigation cluster.  
  - A hands-free speakerphone and handset designed for high-fidelity wideband audio are standard, as is a built-in headset connection. |
| Cisco Unified IP Phone 7962  | The Cisco Unified IP Phone 7962 is a full-featured IP phone with speakerphone and handset designed for wideband audio. It is intended to meet the needs of managers and administrative assistants.  
  - It has six programmable backlit line/feature buttons and four interactive softkeys that guide you through all call features and functions.  
  - The phone has a large, 4-bit grayscale graphical LCD that provides features such as date and time, calling party name, calling party number, digits dialed, and presence information.  
  - The crisp graphic capability of the display allows for the inclusion of higher value, more visibly rich Extensible Markup Language (XML) applications, and support for localization requiring double-byte Unicode encoding for fonts.  
  - A hands-free speakerphone and handset designed for hi-fidelity wideband audio are standard, as is a built-in headset connection and an integrated Ethernet switch. |

Cisco Unified IP Phone 7965 supports SCCP and SIP protocols.  
Cisco Unified IP Phone 7962 supports SCCP and SIP protocols.
<table>
<thead>
<tr>
<th>Cisco Unified IP Phone Model</th>
<th>Description</th>
</tr>
</thead>
</table>
| Cisco Unified IP Phone 7960 | The Cisco Unified IP Phone 7960, a full-featured, six-line business set, supports SCCP and SIP and the following features:  
  • A help (?) button  
  • Six programmable buttons to use as line, speed-dial, or feature buttons  
  • Four fixed buttons for accessing voice-messaging messages, adjusting phone settings, accessing services, and accessing directories  
  • Four softkeys for accessing additional call details and functionality (Softkeys change depending on the call state for a total of 16 softkeys.)  
  • A large LCD display that shows call details and softkey functions  
  • An internal, two-way, full-duplex speakerphone and microphone mute |
| Cisco Unified IP Phone 7945 | The Cisco Unified IP Phone 7945 demonstrates the latest advances in VoIP telephony, including wideband audio support, backlit color display, and an integrated Gigabit Ethernet port.  
This IP phone includes a large, backlit, easy-to-read color display for easy access to communication information, timesaving applications, and features such as date and time, calling party name, calling party number, digits dialed, and presence information.  
The phone provides direct access to two telephone lines (or combination of lines, speed dials, and direct access to telephony features), four interactive softkeys that guide you through call features and functions, and an intuitive four-way (plus Select key) navigation cluster.  
A hands-free speakerphone and handset designed for high-fidelity wideband audio are standard, as is a built-in headset connection.  
Cisco Unified IP Phone 7945 supports SCCP and SIP protocols. |
<table>
<thead>
<tr>
<th>Cisco Unified IP Phone Model</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Unified IP Phone 7942</td>
<td>The Cisco Unified IP Phone 7942 is a full-featured IP phone with speakerphone and handset designed for wideband audio. It is intended to meet the needs of transaction-type workers with significant phone traffic. It has two programmable backlit line/feature buttons and four interactive soft keys that guide you through all call features and functions. The phone has a large, 4-bit grayscale graphical LCD that provides features such as date and time, calling party name, calling party number, digits dialed, and presence information. The crisp graphic capability of the display allows for the inclusion of higher value, more visibly rich Extensible Markup Language (XML) applications, and support for localization requiring double-byte Unicode encoding for fonts. A hands-free speakerphone and handset designed for hi-fidelity wideband audio are standard, as is a built-in headset connection and an integrated Ethernet switch. Cisco Unified IP Phone 7942 supports SCCP and SIP protocols.</td>
</tr>
<tr>
<td>Cisco Unified IP Phone 7940</td>
<td>The Cisco Unified IP Phone 7940, a two-line business set with features similar to the Cisco Unified IP Phone 7960, supports SCCP and SIP and includes the following features:</td>
</tr>
<tr>
<td></td>
<td>• A help (?) button</td>
</tr>
<tr>
<td></td>
<td>• Two programmable buttons to use as line, speed-dial, or feature buttons</td>
</tr>
<tr>
<td></td>
<td>• Four fixed buttons for accessing voice-messaging messages, services, and directories and for adjusting phone settings</td>
</tr>
<tr>
<td></td>
<td>• Four softkeys for accessing additional call details and functionality (Softkeys change depending upon the call state for a total of 16 softkeys.)</td>
</tr>
<tr>
<td></td>
<td>• A large LCD that shows call details and softkey functions</td>
</tr>
<tr>
<td></td>
<td>• An internal, two-way, full-duplex speakerphone and microphone mute</td>
</tr>
<tr>
<td><strong>Cisco Unified IP Phone Model</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>---------------------------------</td>
<td>----------------</td>
</tr>
</tbody>
</table>
| Cisco Unified IP Phone 7931 | The Cisco Unified IP Phone 7931, designed for users who are familiar with traditional key sets, functions much like a digital business phone, allowing users to place and receive phone calls and to access features such as mute, hold, transfer, speed dial, call forward, and more, including:
- Pixel-based backlit display
- 24 configurable line buttons
- Wideband Headset option-disabled by default (should be enabled only if the user headset supports wideband)
- Abbreviated dialing
- Audible Message Waiting Indicator
- Call forward configurable display
- Call forward destination override
- Call Recording
- Directed Call Park
- Do Not Disturb (DND)
- Video support
- Voice Unified system |
| Cisco Unified Wireless IP Phone 7925 | The Cisco Unified Wireless IP Phone 7925 is designed for users in rigorous workspaces as well as general office environments. It supports a wide range of features for enhanced voice communications, quality of service (QoS), and security. Some of the main benefits and highlights are listed here:
- IEEE 802.11 a/b/g radio
- Two-inch color display
- Bluetooth 2.0 support with Enhanced Data Rate (EDR)
- IP54 rated for protection against dust and splashing water
- MIL-STD-810F standard for shock resistance
- Long battery life (up to 240 hours of standby time or 13 hours of talk time)
- Built-in speakerphone for hands-free operation
- Exceptional voice quality with support for wideband audio
- Support for a wide range of applications through XML

Cisco Unified Wireless IP Phone 7925 supports the SCCP protocol. |
Cisco Unified IP Phone Model | Description
--- | ---
Cisco Unified Wireless IP Phone 7921 | The Cisco Unified Wireless IP Phone 7921 supports a host of calling features and voice-quality enhancements. The device is an advanced media IP phone, delivering wideband audio capabilities. In addition to wideband audio, Cisco Unified Wireless IP Phone 7921 supports presence, which enables users in a mobile Wi-Fi environment to view the current status of other users. Because the Cisco Unified Wireless IP Phone 7921G is designed to grow with system capabilities, features will keep pace with new system enhancements. Cisco Unified Wireless IP Phone 7921 supports the SCCP protocol.

Cisco Unified Wireless IP Phone 7920 | The Cisco Wireless IP Phone 7920, which is an easy-to-use IEEE 802.11b wireless IP phone, provides comprehensive voice communication in conjunction with Cisco Unified Communications Manager and Cisco Aironet 1200, 1100, 350, and 340 series of Wi-Fi (IEEE 802.11b) access points. Features include

• A pixel-based display for intuitive access to calling features
• Two softkeys that dynamically present calling options to the user
• A four-way rocker switch that allows easy movement through the displayed information
• Volume control for easy decibel-level adjustments of the handset and ringer when in use

Cisco Unified IP Phone Expansion Module 7914 | Cisco Unified IP Phone Expansion Module 7914 extend the functionality of a Cisco Unified IP Phone by providing 14 additional buttons. To configure these buttons as line or speed dials, use Phone Button Template Configuration.

**Note** You can create the Cisco Unified IP Phone Expansion Module 7914 phone button template by copying the phone button template for the standard Cisco Unified IP Phone model that you are using with your Cisco Unified IP Phone Expansion Module 7914.

The Cisco Unified IP Phone Expansion Module 7914 includes an LCD to identify the function of the button and the line status.

You can daisy chain two Cisco Unified IP Phone Expansion Modules 7914 to provide 28 additional lines or speed-dial and feature buttons.
<table>
<thead>
<tr>
<th><strong>Cisco Unified IP Phone Model</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Unified IP Phone Expansion Module 7915 and Cisco Unified IP Phone Expansion Module 7916</td>
<td>Cisco Unified IP Phone Expansion Module 7915 and 7916 extends the functionality of a Cisco Unified IP Phone by providing 24 additional buttons. To configure these buttons as line or speed dials, use Phone Button Template Configuration. <strong>Note</strong> You create the Cisco Unified IP Phone Expansion Module phone button template by copying the phone button template for the standard Cisco Unified IP Phone model that you are using with your Cisco Unified IP Phone Expansion Module 7915 or 7916. The Cisco Unified IP Phone Expansion Module 7915 and 7916 includes an LCD to identify the function of the button and the line status. You can daisy chain two Cisco Unified IP Phone Expansion Module 7915s or 7916s to provide 48 additional lines or speed-dial and feature buttons.</td>
</tr>
<tr>
<td>Cisco Unified IP Color Key Expansion Module</td>
<td>Cisco Unified IP Color Key Expansion Module extends the functionality of a Cisco Unified IP Phone by providing 36 additional buttons. The programmable buttons can be set up as phone line buttons, speed-dial buttons, or phone feature buttons. To configure these buttons as line buttons, speed dial buttons, or phone features buttons, use the Phone Button Template Configuration. <strong>Note</strong> You create the Cisco Unified IP Color Key Expansion Module phone button template by copying the phone button template for the standard Cisco Unified IP Phone model that you are using with your Cisco Unified IP Color Key Expansion Module. You can attach one Cisco Unified IP Color Key Expansion Module to a Cisco Unified IP Phone 8961 for 36 additional buttons, two Cisco Unified IP Color Key Expansion Modules to a Cisco Unified IP Phone 9951 for 72 additional buttons, and three Cisco Unified IP Color Key Expansion Modules to a Cisco Unified IP Phone 9971 for 108 additional buttons.</td>
</tr>
<tr>
<td>Cisco Unified IP Phone 7911</td>
<td>The Cisco Unified IP Phone 7911, which is a single-line phone that supports a maximum of six calls at the same time, supports SCCP and SIP and provides basic-feature functionality for individuals who conduct low to medium telephone traffic. The Applications Menu button opens up a main applications menu. This phone, which supports inline power, provides an integrated 10/100 Ethernet switch for connectivity to a collocated PC. This phone offers four dynamic softkeys.</td>
</tr>
</tbody>
</table>
## Supported Cisco Unified IP phones

<table>
<thead>
<tr>
<th><strong>Cisco Unified IP Phone Model</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Unified IP Phone 7906</td>
<td>The Cisco Unified IP Phone 7906, which is a single-line phone that supports a maximum of six calls at the same time, supports SCCP and SIP and provides basic-feature functionality for individuals who conduct low to medium telephone traffic. The Applications Menu button opens up a main applications menu. This phone, which supports inline power, provides an integrated 10/100 Ethernet switch for connectivity to a collocated PC. This phone offers four dynamic softkeys.</td>
</tr>
</tbody>
</table>
| Cisco Unified IP Phone 7985     | The Cisco Unified IP Phone 7985G provides business-quality video over the same data network that your computer uses. The video phone provides the same softkey functionality and features as a Cisco Unified IP Phone, which allows you to place and receive calls, put calls on hold, transfer calls, make conference calls, and so on. The Cisco Unified IP Phone 7985G provides the following features:  
  • Color screen  
  • Support for up to eight line or speed-dial numbers  
  • Context-sensitive online help for buttons and feature |
| Cisco Unified IP Conference Station 7937 | The Cisco Unified IP Conference Station 7937 combines state-of-the-art wideband speakerphone conferencing technologies with award-winning Cisco voice communication technologies. The net result is a conference room phone that offers superior wideband voice and microphone quality, with simplified wiring and administrative cost benefits. A full-featured, IP-based, hands-free conference station, the Cisco Unified IP Conference Station 7937 is designed for use on desktops, in conference rooms, and in executive suites. Cisco Unified IP Conference Station 7937 features include:  
  • Superior wideband acoustics with the support of the G.722 wideband codec  
  • Support for IEEE Power over Ethernet (PoE) or the Cisco Power Cube 3  
  • Expanded room coverage up to 30 feet by 40 feet with the optional external microphone kit  
  • Support for a third-party lapel microphone kit1  
  • New larger backlit liquid crystal display (LCD)  
  • Global localization  
Cisco Unified IP Conference Station 7937 supports the SCCP protocol. |
### Supported Cisco Unified IP phones

<table>
<thead>
<tr>
<th><strong>Cisco Unified IP Phone Model</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
</table>
| **Cisco Unified IP Conference Station 7936** | The Cisco Unified IP Conference Station 7936, a full-featured, IP-based, hands-free conference station for use on desktops, in offices, and in small- to medium-sized conference rooms, includes the following features:  
  - Three softkeys and menu navigation keys that guide a user through call features and functions including available features Call Park, Call Pickup, Group Call Pickup, Transfer, and Conference (Ad Hoc and Meet-Me).  
  - An LCD that indicates the date and time, calling party name, calling party number, digits dialed, feature, and line status  
  - A digitally tuned speaker and three microphones that allow conference participants to move around while speaking  
  - Microphone mute  
  - Ability to add external microphones to support larger rooms |
| **Cisco IP Conference Station 7935** | The Cisco IP Conference Station 7935, a full-featured, IP-based, hands-free conference station for use on desktops, in offices, and in small- to medium-sized conference rooms, includes the following features:  
  - Three softkeys and menu navigation keys that guide a user through call features and functions  
    Available features include Call Park, Call Pickup, Group Call Pickup, Transfer, and Conference (Ad Hoc and Meet-Me).  
  - An LCD that indicates the date and time, calling party name, calling party number, digits dialed, feature, and line status  
  - A digitally tuned speaker and three microphones that allow conference participants to move around while speaking  
  - Microphone mute |
The Cisco Unified IP Phone 6961 is a new and innovative IP endpoint that delivers affordable, business-grade voice communication and video communication services to customers worldwide.

- The Cisco Unified IP Phone 6961 supports 12 lines, paper label inserts for line and feature descriptions along with a full-duplex speakerphone for a more productive, more flexible, and easier-to-use endpoint experience.
- Single-call per-line appearance is introduced, delivering traditional telephony-like user experience for customers who seek this type of call interaction for their users.
- Fixed keys for hold, transfer, and conference; tri-color LED line and feature keys also make the endpoint simpler and easier to use.
- Right-to-left language presentation is also supported on the displays, addressing the language localization needs of global customers.
- The Cisco Unified IP Phone 6961 is also energy-efficient and eco-friendly, in support of customer green initiatives. A Deep-Sleep option provides energy savings. With this option, the Cisco Unified IP Phone 6961 consumes up to 50 percent less power in off-hours versus when the phone is idle during normal business hours. In addition, the Cisco Unified IP Phone 6961 employs use of both recyclable and reground plastics for a more earth-responsible solution.

Cisco Unified IP Phone 6961 supports the SCCP and SIP protocols.

<table>
<thead>
<tr>
<th>Cisco Unified IP Phone Model</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Unified IP Phone 6961</td>
<td>The Cisco Unified IP Phone 6961 is a new and innovative IP endpoint that delivers affordable, business-grade voice communication and video communication services to customers worldwide.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Cisco Unified IP Phone Model</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Unified IP Phone 6961</td>
<td>The Cisco Unified IP Phone 6961 is a new and innovative IP endpoint that delivers affordable, business-grade voice communication and video communication services to customers worldwide.</td>
</tr>
</tbody>
</table>

- The Cisco Unified IP Phone 6961 supports 12 lines, paper label inserts for line and feature descriptions along with a full-duplex speakerphone for a more productive, more flexible, and easier-to-use endpoint experience.
- Single-call per-line appearance is introduced, delivering traditional telephony-like user experience for customers who seek this type of call interaction for their users.
- Fixed keys for hold, transfer, and conference; tri-color LED line and feature keys also make the endpoint simpler and easier to use.
- Right-to-left language presentation is also supported on the displays, addressing the language localization needs of global customers.
- The Cisco Unified IP Phone 6961 is also energy-efficient and eco-friendly, in support of customer green initiatives. A Deep-Sleep option provides energy savings. With this option, the Cisco Unified IP Phone 6961 consumes up to 50 percent less power in off-hours versus when the phone is idle during normal business hours. In addition, the Cisco Unified IP Phone 6961 employs use of both recyclable and reground plastics for a more earth-responsible solution.

Cisco Unified IP Phone 6961 supports the SCCP and SIP protocols.
The Cisco Unified IP Phone 6941 is an innovative IP endpoint that delivers affordable, business-grade voice communication and support for video communications services to customers worldwide.

- The Cisco Unified IP Phone 6941 supports four lines and a full-duplex speakerphone for a more productive, more flexible, and easier-to-use endpoint experience.
- The phone supports single-call per-line appearance, offering traditional telephony-like user experience for customers who seek this type of call interaction for their users.
- Fixed keys for hold, transfer, and conference; tri-color LED line and feature keys also make the phone simpler and easier to use.
- Right-to-left language presentation is also supported on the displays, addressing the language localization needs of global customers.
- The Cisco Unified IP Phone 6941 is also energy-efficient and eco-friendly, in support of customer green initiatives. A Deep-Sleep option provides energy savings. With this option, the phone consumes up to 50 percent less power in off-hours versus when the phone is idle during normal business hours. In addition, reground and recyclable plastics deliver a more earth-responsible solution.

Cisco Unified IP Phone 6941 supports the SCCP and SIP protocols.

<table>
<thead>
<tr>
<th>Cisco Unified IP Phone Model</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Unified IP Phone 6941</td>
<td>The Cisco Unified IP Phone 6941 is an innovative IP endpoint that delivers affordable, business-grade voice communication and support for video communications services to customers worldwide. The Cisco Unified IP Phone 6941 supports four lines and a full-duplex speakerphone for a more productive, more flexible, and easier-to-use endpoint experience. The phone supports single-call per-line appearance, offering traditional telephony-like user experience for customers who seek this type of call interaction for their users. Fixed keys for hold, transfer, and conference; tri-color LED line and feature keys also make the phone simpler and easier to use. Right-to-left language presentation is also supported on the displays, addressing the language localization needs of global customers. The Cisco Unified IP Phone 6941 is also energy-efficient and eco-friendly, in support of customer green initiatives. A Deep-Sleep option provides energy savings. With this option, the phone consumes up to 50 percent less power in off-hours versus when the phone is idle during normal business hours. In addition, reground and recyclable plastics deliver a more earth-responsible solution. Cisco Unified IP Phone 6941 supports the SCCP and SIP protocols.</td>
</tr>
</tbody>
</table>
### Supported Cisco Unified IP phones

<table>
<thead>
<tr>
<th>Cisco Unified IP Phone Model</th>
<th>Description</th>
</tr>
</thead>
</table>
| Cisco Unified IP Phone 6921 | The Cisco Unified IP Phone 6921 is an innovative endpoint that delivers affordable, business-grade voice communications and support for video communications services to customers worldwide.  

- The Cisco Unified IP Phone 6921 supports two lines and offers a full-duplex speakerphone for a more productive, more flexible, and easier-to-use endpoint experience.  

- The phone supports single-call per-line appearance, offering traditional telephony-like user experience for customers who seek this type of call interaction for their users.  

- Fixed keys for hold, transfer, and conference; tri-color LED line and feature keys also make the phone simpler and easier to use.  

- Right-to-left language presentation is also supported on the displays, addressing the language localization needs of global customers.  

- The Cisco Unified IP Phone 6921 is also energy-efficient and eco-friendly, in support of customer green initiatives. A Deep-Sleep option provides energy savings. With this option, the phone consumes up to 50 percent less power in off-hours versus when the phone is idle during normal business hours. In addition, reground and recyclable plastics deliver a more earth-responsible solution.  

Cisco Unified IP Phone 6921 supports the SCCP and SIP protocols.
<table>
<thead>
<tr>
<th><strong>Cisco Unified IP Phone Model</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
</table>
| Cisco Unified IP Phone 6911     | The Cisco Unified IP Phone 6911 is a single-line endpoint delivering affordable access to Cisco voice communication services. It is an ideal solution for light communication requirements. Examples include classrooms, manufacturing floors, or employees in cubicles or teleworking from home.  
  - The Cisco Unified IP Phone 6911 supports two incoming calls with a single-line endpoint.  
  - A full-duplex speakerphone is included in the design, which provides a more productive, flexible, and easier-to-use endpoint experience.  
  - Integrated IEEE 10/100 Ethernet switch ports support connection to a co-located PC while reducing cabling infrastructure and administration costs.  
  - The phone includes fixed keys for hold, transfer, conference, redial, and voicemail, making the phone simple and easy-to-use. In addition, a programmable feature key is supported for quick access to advanced communication services.  
  - Tri-color LED illuminates on the line key to provide quick call-state indication at a glance.  
  - The Cisco Unified IP Phone 6911 is also eco-friendly, taking advantage of reground and recyclable plastics to deliver a more earth-responsible solution.  
  Cisco Unified IP Phone 6911 supports the SCCP and SIP protocols. |
| Cisco Unified IP Phone 6901     | The Cisco Unified IP Phone 6901 is a single-line endpoint delivering cost-effective access to Cisco Unified Communications. Designed with a trimline-like low profile, the phone is an ideal solution for lobbies, hallways, elevators, hotel bathrooms, or other settings that have an occasional need for voice communications services.  
  - The phone supports two incoming calls with call-waiting service.  
  - Fixed feature keys provide one-touch access to Hold, Redial, and Call Waiting.  
  - Transfer and Conference can be supported by using the hook-switch similar to that of traditional analog phones.  
  - The Cisco Unified IP Phone 6901 is an earth-friendly solution. As with the other Cisco Unified IP Phone 6900 Series endpoints, the Cisco Unified IP Phone 6901 takes advantage of reground and recyclable plastics for a more earth-responsible solution.  
  Cisco Unified IP Phone 6901 supports the SCCP and SIP protocols. |
<table>
<thead>
<tr>
<th>Cisco Unified IP Phone Model</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Unified SIP Phone 3951</td>
<td>Be aware that the Cisco Unified SIP Phone 3951, a low-end phone that runs SIP, is available only in Asia Pacific and Latin American countries. For more information, contact your Cisco representative.</td>
</tr>
</tbody>
</table>

**Cisco E20**

The Cisco E20 reinvents the desk phone by merging voice, video, and collaboration into one device. A highly scalable solution for enterprise mass deployment, users will immediately see the benefits of increased productivity and daily collaboration.

The Cisco E20 offers the following capabilities:

- Intuitive user interface and keypad for quick access to all IP phone and video services
- Familiar telephony features such as Hold, Transfer, Resume, and Conference
- Handset, headset (bluetooth), speakerphone flexibility
- Navigation cluster with select button
- Message waiting indicator/button
- 5 contextual softkeys
- USB picture frame
- High-resolution camera with integrated privacy shutter
- DVD quality, w448p video resolution
- 10.6” wide format LCD display with WXGA resolution
- Video standards and resolutions: H.264, H.263, and H.263+ from SIF up to w448p
- Bandwidth up to 1152 kbps

The Cisco E20 supports SIP.
Third-party SIP endpoints

Cisco Unified Communications Manager supports a variety of third-party SIP endpoints, which are configured in Cisco Unified Communications Manager Administration, Phone Configuration.

Cisco Unified Communications Manager requires user licenses. These licenses get configured in Cisco Unified Communications Manager Administration, License Configuration. When acquiring user licenses, the administrator purchases one user license, called user connect license (UCL), for each user. License Configuration uses device license units (DLU). For example, if there are three generic desktop video endpoint users (3 UCLs), License Configuration would need 18 DLUs (3 UCL x 6 DLU = 18 DLU).

When using Phone Configuration to add a third-party SIP endpoint, the following device phone types are available:

- Third-Party SIP Device (Advanced)-This eight-line SIP device is an RFC3261-compliant phone that is running SIP from third-party companies; this device requires 6 DLUs.
- Third-Party SIP Device (Basic)-This one-line SIP device is an RFC3261-compliant phone that is running SIP from third-party companies; this device requires 3 Device License Units (DLUs).
- Third-Party AS-SIP Device - Third-party AS-SIP endpoints are compliant with Assured Services SIP, which includes MLPP, DSCP, TLS/SRTP, and IPv6 requirements.
- Generic Desktop Video Endpoint-This SIP device supports video, security, configurable trust, and Cisco extensions; this device requires 6 DLUs. This device supports 8 lines; the maximum number of calls and busy trigger for each line is 4 and 2, respectively.
- Generic Single Screen Room System-This SIP device supports single screen telepresence (room systems), video, security, configurable trust, and Cisco extensions; this device requires 6 DLUs. This device supports 8 lines; the maximum number of calls and busy trigger for each line is 4 and 2, respectively.
- Generic Multiple Screen Room System-This SIP device supports multiple screen telepresence (room systems), video, security, configurable trust, and Cisco extensions; this device requires 6 DLUs. This device supports 8 lines; the maximum number of calls and busy trigger for each line is 4 and 2, respectively.

H.323 clients and CTI ports

Cisco Unified Communications Manager Administration enables you to configure software-based devices such as H.323 clients and CTI ports. Software-based Cisco Unified Communications Manager applications such as Cisco IP Softphone, Cisco Unified Communications Manager Auto-Attendant, and Cisco IP Interactive Voice Response (IVR) use CTI ports that are virtual devices.
H.323 clients include Microsoft NetMeeting devices.

You configure H.323 clients and CTI ports through the Phone Configuration window in Cisco Unified Communications Manager Administration like you do phones, but they often require fewer configuration settings.

---

**Note**

Cisco recommends that you do not configure CTI ports or devices that use TAPI applications in a line group.

For information on H.323 clients and shared line appearances, see the [Shared line appearance, on page 193](#).

---

## CTI remote device setup

The CTI Remote Device type enables third-party desktop clients to receive incoming calls, initiate Dial via Office reverse calls, and perform mid-call features. Consult the third-party vendor documentation to confirm support for this device type.

In Cisco Unified Communications Manager Administration, use the **Device > Phone** menu path to configure CTI Remote Device. CTI Remote devices configuration specifies a set of parameters that apply to all the CTI Remote Devices for the user.

CTI Remote Device type represents the users remote device(s), similar to the Mobile Communicator device type. You can add a Remote Destination for a CTI Remote Device. The Remote Destination associated with the CTI Remote Device specifies the number to reach the Remote Device. The maximum number of Remote Destinations that you can configure for a CTI Remote Device is dependent on the Remote Destination limit set for the Owner User ID. By default, this value is set to 4.

### Tips About Configuring CTI Remote Devices

You can add a maximum of five Directory Numbers to the CTI Remote Device. To register a CTI Remote Device, add a Directory Number to that device. You cannot register a CTI Remote Device without a Directory Number.

### Using the GUI

For instructions on how to use the Cisco Unified Communications Manager Administration Graphical User Interface (GUI) to find, delete, configure, or copy records, see the *Cisco Unified Communications Manager Administration Guide* and its subsections, which explain how to use the GUI and detail the functions of the buttons and icons.

### Configuration Settings Table

The following table describes the available settings to configure a CTI remote device through the Phone Configuration Settings window.

#### Table 42: CTI Remote Device Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CTI Remote Device Information</td>
<td></td>
</tr>
<tr>
<td>Device Information</td>
<td></td>
</tr>
</tbody>
</table>
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Registration</td>
<td>Specifies the registration status of the CTI Remote Device.</td>
</tr>
<tr>
<td>Device Status</td>
<td>Specifies if the device is active or inactive.</td>
</tr>
<tr>
<td>Device Trust</td>
<td>Specifies if the device is trusted.</td>
</tr>
<tr>
<td>Active Remote Destination</td>
<td>Specifies the Remote Destination which is active. The CTI client can specific one remote destination as 'active' at any one given time. Incoming calls and Dial via Office (DVO) calls are routed to the active remote destination.</td>
</tr>
<tr>
<td>Owner User ID</td>
<td>From the drop-down list box, choose the user ID of the assigned phone user. The user ID gets recorded in the call detail record (CDR) for all calls made from this device.</td>
</tr>
<tr>
<td>Device Name</td>
<td>Specifies the name for the CTI Remote Device which is automatically populated based on the Owner User ID.</td>
</tr>
<tr>
<td>Description</td>
<td>The format of the device name is CTIRD&lt;OwnerUserID&gt; by default.</td>
</tr>
<tr>
<td></td>
<td>You can also edit the device name. The device name can comprise up to 15 characters. Valid characters include letters, numbers, dashes, dots (periods), spaces, and underscores.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a text description of the CTI remote device.</td>
</tr>
<tr>
<td></td>
<td>This field can comprise up to 128 characters. You can use all characters except quotes (&quot;), close angle bracket (&gt;), open angle bracket (&lt;), backslash (), ampersand (&amp;), and percent sign (%).</td>
</tr>
<tr>
<td>Device Pool</td>
<td>Select the device pool which defines the common characteristics for CTI remote devices.</td>
</tr>
<tr>
<td></td>
<td>For more information on how to configure the device pool, see Device Pool Configuration Settings.</td>
</tr>
<tr>
<td>Calling Search Space</td>
<td>Using the drop-down list box, choose the calling search space or leave the calling search space as the default of &lt;None&gt;.</td>
</tr>
<tr>
<td>User Hold MOH Audio Source</td>
<td>Using the drop-down list box, choose the audio source to use for music on hold (MOH) when a user initiates a hold action.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Network Hold MOH Audio Source</td>
<td>Using the drop-down list box, choose the audio source to use for MOH when the network initiates a hold action.</td>
</tr>
<tr>
<td>Location</td>
<td>Using the drop-down list box, choose the location that is associated with the phones and gateways in the device pool.</td>
</tr>
<tr>
<td>Calling Party Transformation CSS</td>
<td>This setting allows you to localize the calling party number on the device. Make sure that the Calling Party Transformation CSS that you choose contains the calling party transformation pattern that you want to assign to this device.</td>
</tr>
<tr>
<td>Ignore Presentation Indicators (internal calls only)</td>
<td>Check this check box to configure call display restrictions on a call-by-call basis. When this check box is checked, Cisco Unified CM ignores any presentation restriction that is received for internal calls.</td>
</tr>
</tbody>
</table>

**Call Routing Information**

**Inbound/Outbound Calls Information**

<table>
<thead>
<tr>
<th>Calling Party Transformation CSS</th>
<th>This setting allows you to localize the calling party number on the device. Make sure that the Calling Party Transformation CSS that you choose contains the calling party transformation pattern that you want to assign to this device.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Device Pool Calling Party Transformation CSS</td>
<td>To use the Calling Party Transformation CSS that is configured in the device pool that is assigned to this device, check this check box. If you do not check this check box, the device uses the Calling Party Transformation CSS that you configured in the Trunk Configuration window.</td>
</tr>
</tbody>
</table>

**Protocol Specific Information**

| Presence Group                                      | Configure this field with the Presence feature. If you are not using this application user with presence, leave the default (None) setting for presence group. From the drop-down list box, choose a Presence group for the application user. The group selected specifies the destinations that the application user, such as IPMASysUser, can monitor. |

---

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Hold MOH Audio Source</td>
<td>Using the drop-down list box, choose the audio source to use for MOH when the network initiates a hold action.</td>
</tr>
<tr>
<td>Location</td>
<td>Using the drop-down list box, choose the location that is associated with the phones and gateways in the device pool.</td>
</tr>
<tr>
<td>Calling Party Transformation CSS</td>
<td>This setting allows you to localize the calling party number on the device. Make sure that the Calling Party Transformation CSS that you choose contains the calling party transformation pattern that you want to assign to this device.</td>
</tr>
<tr>
<td>Ignore Presentation Indicators (internal calls only)</td>
<td>Check this check box to configure call display restrictions on a call-by-call basis. When this check box is checked, Cisco Unified CM ignores any presentation restriction that is received for internal calls.</td>
</tr>
</tbody>
</table>

**Call Routing Information**

**Inbound/Outbound Calls Information**

<table>
<thead>
<tr>
<th>Calling Party Transformation CSS</th>
<th>This setting allows you to localize the calling party number on the device. Make sure that the Calling Party Transformation CSS that you choose contains the calling party transformation pattern that you want to assign to this device.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Device Pool Calling Party Transformation CSS</td>
<td>To use the Calling Party Transformation CSS that is configured in the device pool that is assigned to this device, check this check box. If you do not check this check box, the device uses the Calling Party Transformation CSS that you configured in the Trunk Configuration window.</td>
</tr>
</tbody>
</table>

**Protocol Specific Information**

| Presence Group                                      | Configure this field with the Presence feature. If you are not using this application user with presence, leave the default (None) setting for presence group. From the drop-down list box, choose a Presence group for the application user. The group selected specifies the destinations that the application user, such as IPMASysUser, can monitor. |
Supported with the Presence feature, the SUBSCRIBE calling search space determines how Cisco Unified Communications Manager routes presence requests that come from the end user. This setting allows you to apply a calling search space separate from the call-processing search space for presence (SUBSCRIBE) requests for the end user.

From the drop-down list box, choose the SUBSCRIBE calling search space to use for presence requests for the end user. All calling search spaces that you configure in Cisco Unified Communications Manager Administration display in the SUBSCRIBE Calling Search Space drop-down list box.

If you do not select a different calling search space for the end user from the drop-down list, the SUBSCRIBE calling search space defaults to None.

To configure a SUBSCRIBE calling search space specifically for this purpose, you configure a calling search space as you do all calling search spaces.

Rerouting Calling Search Space

From the drop-down list box, choose a calling search space to use for rerouting.

The rerouting calling search space of the referrer gets used to find the route to the refer-to target. When the Refer fails due to the rerouting calling search space, the Refer Primitive rejects the request with the “405 Method Not Allowed” message.

The redirection (3xx) primitive and transfer feature also uses the rerouting calling search space to find the redirect-to or transfer-to target.

Do Not Disturb Information

Do Not Disturb

Check this check box to enable Do Not Disturb on the remote device.

DND Option

When you enable DND on the phone, Call Reject option specifies that no incoming call information gets presented to the user. Depending on how you configure the DND Incoming Call Alert parameter, the phone may play a beep or display a flash notification of the call.

After you configure the CTI Remote Device, you can configure the associated remote destination. Click Device > Phone > CTI Remote Device > Associated Remote Destinations > Add a New Remote Destination to add and associate the remote destination with the CTI Remote Device.
You can configure a maximum of four unique Remote Destinations to associate with the CTI Remote Device.

When the Remote Destination is configured through the CTI Remote Device configuration window, the following parameters are altered.

- **Mobile Phone**—This function is disabled by default. The field cannot be edited and is not visible on the Administrative Interface.
- **Enable Mobile Connect**—This function is enabled by default. The field cannot be edited and is not visible on the Administrative Interface.

You can also configure the remote destination from Device > Remote Destination window.

You cannot edit these two fields while you configure the Remote Destination through the CTI Remote Device configuration window.

### Client Services Framework setup

In Cisco Unified Communications Manager Administration, use the **Device > Phone** menu path to configure the Cisco Unified Client Services Framework device.

This section describes how to configure a Cisco Unified Client Services Framework device through the Phone Configuration Settings window.

For instructions on how to use the Cisco Unified Communications Manager Administration Graphical User Interface (GUI) to find, delete, configure, or copy records, see the *Cisco Unified Communications Manager Administration Guide* and its subsections, which explain how to use the GUI and detail the functions of the buttons and icons.

### Configuration Settings Table

The following table describes the available settings in the Client Services Framework Configuration window.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Unified Client Services Framework Information</td>
<td></td>
</tr>
</tbody>
</table>
### Field | Description
--- | ---
Device Protocol | Specifies the protocol used to the Cisco Unified Client Services Framework.
Active Remote Destination | Specifies the Remote Destination which is active. The CSF client can specific one remote destination as 'active' at any one given time. Incoming calls and Dial via Office (DVO) calls are routed to the active remote destination.

### Device Information
Device Status | Specifies if the device is active or inactive.
Device Trust | Specifies if the device is trusted or not.
Device Name | Enter a text name for the Client Services Framework. This name can comprise up to 50 characters. Valid characters include letters, numbers, dashes, dots (periods), spaces, and underscores.
Description | Enter a text description of the Client Services Framework. This field can comprise up to 128 characters. You can use all characters except quotes ("), close angle bracket (>), open angle bracket (<), backslash (\), ampersand (&), and percent sign (%).
Device Pool | Select the device pool which defines the common characteristics for Client Services Framework. For more information on how to configure the device pool, see Device Pool Configuration Settings.
Common Device Configuration | Using the drop-down list box, choose the common device configuration to which you want this trunk assigned. The common device configuration includes the attributes (services or features) that are associated with a particular user. Common device configurations are configured in the Common Device Configuration window.
Phone Button Template | Using the drop-down list box, choose the appropriate phone button template. The phone button template determines the configuration of buttons on a phone and identifies which feature (line, speed dial, and so on) is used for each button.
Common Phone Profile | Using the drop-down list box, choose the common phone profile to specify the data that is required by the Cisco TFTP.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Calling Search Space      | Choose the calling search space to be used for routing Mobile Voice Access or Enterprise Feature Access calls.  
**Note** This calling search space setting applies only when you are routing calls from the remote destination, which specifies the outbound call leg to the dialed number for Mobile Voice Access and Enterprise Feature Access calls. |
| AAR Calling Search Space  | Choose the appropriate calling search space for the device to use when automated alternate routing (AAR) is performed. The AAR calling search space specifies the collection of route partitions that are searched to determine how to route a collected (originating) number that is otherwise blocked due to insufficient bandwidth. |
| Media Resource Group List | Choose the appropriate Media Resource Group List. A Media Resource Group List comprises a prioritized grouping of media resource groups. An application chooses the required media resource, such as a Music On Hold server, from the available media resources according to the priority order that is defined in a Media Resource Group List.  
If you choose <none>, Cisco Unified Communications Manager uses the Media Resource Group that is defined in the device pool. |
<p>| User Hold MOH Audio Source| Using the drop-down list box, choose the audio source to use for music on hold (MOH) when a user initiates a hold action.                                                                                           |
| Network Hold MOH Audio Source| Using the drop-down list box, choose the audio source to use for MOH when the network initiates a hold action.                                                                                                     |
| Location                  | Using the drop-down list box, choose the location that is associated with the phones and gateways in the device pool.                                                                                           |
| AAR Group                 | Choose the automated alternate routing (AAR) group for this device. The AAR group provides the prefix digits that are used to route calls that are otherwise blocked due to insufficient bandwidth. An AAR group setting of None specifies that no rerouting of blocked calls will be attempted. |</p>
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| User Locale         | From the drop-down list box, choose the locale that is associated with the CTI route point. The user locale identifies a set of detailed information to support users, including language and font. Cisco Unified Communications Manager makes this field available only for CTI route points that support localization.  
**Note** If no user locale is specified, Cisco Unified Communications Manager uses the user locale that is associated with the device pool.  
**Note** If the users require that information be displayed (on the phone) in any language other than English, verify that the locale installer is installed before configuring user locale. See the Cisco Unified Communications Manager locale installer that is in the Cisco Unified Communications Operating System Administration Guide. |
| Network Locale      | From the drop-down list box, choose the locale that is associated with the gateway. The network locale identifies a set of detailed information to support the hardware in a specific location. The network locale contains a definition of the tones and cadences that the device uses in a specific geographic area.  
**Note** Choose only a network locale that is already installed and that the associated devices support. The list contains all available network locales for this setting, but not all are necessarily installed. If the device is associated with a network locale that it does not support in the firmware, the device will fail to come up. |
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Device Mobility Mode  | From the drop-down list box, turn the device mobility feature on or off for this device or choose Default to use the default device mobility mode. Default setting uses the value for the Device Mobility Mode service parameter for the device. Click **View Current Device Mobility Settings** to display the current values of these device mobility parameters:  
  - Cisco Unified Communications Manager Group  
  - Roaming Device Pool  
  - Location  
  - Region  
  - Network Locale  
  - AAR Group  
  - AAR Calling Search Space  
  - Device Calling Search Space  
  - Media Resource Group List  
  - SRST  
  For more configuration information, see “Device Mobility” in the *Cisco Unified Communications Manager Features and Services Guide*. |
| Owner User ID         | From the drop-down list box, choose the user ID of the assigned phone user. The user ID gets recorded in the call detail record (CDR) for all calls made from this device.  
  **Note**  Do not configure this field if you are using extension mobility. Extension mobility does not support device owners. |
| Mobility User ID      | From the drop-down list box, choose the user ID of the person to whom this dual-mode phone is assigned.  
  **Note**  The Mobility User ID configuration gets used for the Mobile Connect and Mobile Voice Access features for dual-mode phones.  
  **Note**  The Owner User ID and Mobility User ID can differ. |
| Primary Phone         | Choose the physical phone that will be associated with the application, such as IP communicator or Cisco Unified Personal Communicator. When you choose a primary phone, the application consumes fewer device license units and is considered an "adjunct" license (to the primary phone). See “Licensing” in the *Cisco Unified Communications Manager Features and Services Guide*. |
From the drop-down list box, enable or disable whether Cisco Unified CM inserts a trusted relay point (TRP) device with this media endpoint. Choose one of the following values:

- Default—If you choose this value, the device uses the Use Trusted Relay Point setting from the common device configuration with which this device associates.

- Off—Choose this value to disable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates.

- On—Choose this value to enable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates.

A Trusted Relay Point (TRP) device designates an MTP or transcoder device that is labeled as Trusted Relay Point. Cisco Unified CM places the TRP closest to the associated endpoint device if more than one resource is needed for the endpoint (for example, a transcoder or RSVPAgent).

If both TRP and MTP are required for the endpoint, TRP gets used as the required MTP. See the “TRP Insertion” in Cisco Unified Communications Manager System Guide for details of call behavior.

If both TRP and RSVP Agent are needed for the endpoint, Cisco Unified CM first tries to find an RSVP Agent that can also be used as a TRP.

If both TRP and transcoder are needed for the endpoint, Cisco Unified CM first tries to find a transcoder that is also designated as a TRP.

See the “Trusted Relay Point” section and its subtopics in the “Media Resource Management” chapter of the Cisco Unified Communications Manager System Guide for a complete discussion of network virtualization and trusted relay points.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Use Trusted Relay Point | From the drop-down list box, enable or disable whether Cisco Unified CM inserts a trusted relay point (TRP) device with this media endpoint. Choose one of the following values:  
  - Default—If you choose this value, the device uses the Use Trusted Relay Point setting from the common device configuration with which this device associates.  
  - Off—Choose this value to disable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates.  
  - On—Choose this value to enable the use of a TRP with this device. This setting overrides the Use Trusted Relay Point setting in the common device configuration with which this device associates.  
  A Trusted Relay Point (TRP) device designates an MTP or transcoder device that is labeled as Trusted Relay Point. Cisco Unified CM places the TRP closest to the associated endpoint device if more than one resource is needed for the endpoint (for example, a transcoder or RSVPAgent).  
  If both TRP and MTP are required for the endpoint, TRP gets used as the required MTP. See the “TRP Insertion” in Cisco Unified Communications Manager System Guide for details of call behavior.  
  If both TRP and RSVP Agent are needed for the endpoint, Cisco Unified CM first tries to find an RSVP Agent that can also be used as a TRP.  
  If both TRP and transcoder are needed for the endpoint, Cisco Unified CM first tries to find a transcoder that is also designated as a TRP.  
  See the “Trusted Relay Point” section and its subtopics in the “Media Resource Management” chapter of the Cisco Unified Communications Manager System Guide for a complete discussion of network virtualization and trusted relay points. |
### Field | Description
--- | ---
Always Use Prime Line | From the drop-down list box, choose one of the following options:

- **Off**—When the phone is idle and receives a call on any line, the phone user answers the call from the line on which the call is received.

- **On**—When the phone is idle (off hook) and receives a call on any line, the primary line gets chosen for the call. Calls on other lines continue to ring, and the phone user must select those other lines to answer these calls.

- **Default**—Cisco Unified Communications Manager uses the configuration from the Always Use Prime Line service parameter, which supports the Cisco Call Manager service.

Always Use Prime Line for Voice Message | From the drop-down list box, choose one of the following options:

- **On**—If the phone is idle, the primary line on the phone becomes the active line for retrieving voice messages when the phone user presses the Messages button on the phone.

- **Off**—If the phone is idle, pressing the Messages button on the phone automatically dials the voice-messaging system from the line that has a voice message. Cisco Unified CM always selects the first line that has a voice message. If no line has a voice message, the primary line gets used when the phone user presses the Messages button.

- **Default**—Cisco Unified CM uses the configuration from the Always Use Prime Line for Voice Message service parameter, which supports the Cisco Call Manager service.

Calling Party Transformation CSS | This setting allows you to localize the calling party number on the device. Make sure that the Calling Party Transformation CSS that you choose contains the calling party transformation pattern that you want to assign to this device.

**Tip** Before the call occurs, the device must apply the transformation by using digit analysis. If you configure the Calling Party Transformation CSS as None, the transformation does not match and does not get applied. Ensure that you configure the Calling Party Transformation Pattern in a non-null partition that is not used for routing.

Geolocation | From the drop-down list box, choose a geolocation.

You can choose the Unspecified geolocation, which designates that this device does not associate with a geolocation.

You can also choose a geolocation that has been configured with the **System > Geolocation** Configuration menu option.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ignore Presentation Indicators (internal calls only)</td>
<td>Check this check box to configure call display restrictions on a call-by-call basis. When this check box is checked, Cisco Unified CM ignores any presentation restriction that is received for internal calls. Use this configuration in combination with the calling line ID presentation and connected line ID presentation configuration at the translation pattern level. Together, these settings allow you to configure call display restrictions to selectively present or block calling and/or connected line display information for each call.</td>
</tr>
<tr>
<td>Allow Control of Device from CTI</td>
<td>Check this check box to allow CTI to control and monitor this device. If the associated directory number specifies a shared line, the check box should be enabled as long as at least one associated device specifies a combination of device type and protocol that CTI supports.</td>
</tr>
<tr>
<td>Logged Into Hunt Group</td>
<td>This check box, which gets checked by default for all phones, indicates that the phone is currently logged in to a hunt list (group). When the phone gets added to a hunt list, the administrator can log the user in or out by checking (and unchecking) this check box. Users use the softkey on the phone to log their phone in or out of the hunt list.</td>
</tr>
</tbody>
</table>
If you are experiencing delayed connect times over SCCP pipes to remote sites, check the Remote Device checkbox in the Phone Configuration window. Checking this check box tells Cisco Unified CM to allocate a buffer for the phone device when it registers and to bundle SCCP messages to the phone.

**Tip** Because this feature consumes resources, be sure to check this check box only when you are experiencing signaling delays for phones that are running SCCP. Most users do not require this option.

Cisco Unified CM sends the bundled messages to the phone when the station buffer is full, as soon as it receives a media-related message, or when the Bundle Outbound SCCP Messages timer expires.

To specify a setting other than the default setting (100 msec) for the Bundle Outbound SCCP Messages timer, configure a new value in the Service Parameters Configuration window for the Cisco CallManager service. Although 100 msec specifies the recommended setting, you may enter 15 msec to 500 msec.

The phone must support SCCP version 9 to use this option. The following phones do not support SCCP message optimization: Cisco Unified IP Phone 7935/7936. This feature may require a phone reset after update.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote Device</td>
<td>If you are experiencing delayed connect times over SCCP pipes to remote sites, check the Remote Device check box in the Phone Configuration window. Checking this check box tells Cisco Unified CM to allocate a buffer for the phone device when it registers and to bundle SCCP messages to the phone.</td>
</tr>
<tr>
<td>Require off-premise location</td>
<td>Check this check box to allow CTI device be available at an off-premise locations.</td>
</tr>
</tbody>
</table>

**Call Routing Information**

**Inbound/Outbound Calls Information**

**Calling Party Transformation CSS**

This setting allows you to localize the calling party number on the device. Make sure that the Calling Party Transformation CSS that you choose contains the calling party transformation pattern that you want to assign to this device.

**Use Device Pool Calling Party Transformation CSS**

To use the Calling Party Transformation CSS that is configured in the device pool that is assigned to this device, check this check box. If you do not check this check box, the device uses the Calling Party Transformation CSS that you configured in the Trunk Configuration window.

**Protocol Specific Information**
### Field | Description
--- | ---
Packet Capture Mode | This setting exists for troubleshooting encryption only; packet capturing may cause high CPU usage or call-processing interruptions. Choose one of the following options from the drop-down list box:

- **None**—This option, which serves as the default setting, indicates that no packet capturing is occurring. After you complete packet capturing, configure this setting.

- **Batch Processing Mode**—Cisco Unified CM writes the decrypted or nonencrypted messages to a file, and the system encrypts each file. On a daily basis, the system creates a new file with a new encryption key. Cisco Unified CM, which stores the file for seven days, also stores the keys that encrypt the file in a secure location. Cisco Unified CM stores the file in the PktCap virtual directory. A single file contains the time stamp, source IP address, source IP port, destination IP address, packet protocol, message length, and the message.

  The TAC debugging tool uses HTTPS, administrator username and password, and the specified day to request a single encrypted file that contains the captured packets. Likewise, the tool requests the key information to decrypt the encrypted file.

  For more information on packet capturing, see the *Troubleshooting Guide for Cisco Unified Communications Manager*.

Packet Capture Duration | This setting exists for troubleshooting encryption only; packet capturing may cause high CPU usage or call-processing interruptions.

  This field specifies the maximum number of minutes that is allotted for one session of packet capturing. The default setting equals 0, although the range exists from 0 to 300 minutes.

  To initiate packet capturing, enter a value other than 0 in the field. After packet capturing completes, the value, 0, displays.

  For more information on packet capturing, see the *Cisco Unified Communications Manager Troubleshooting Guide*.

Presence Group | Configure this field with the Presence feature.

**Note** If you are not using this application user with presence, leave the default (None) setting for presence group. From the drop-down list box, choose a Presence group for the application user. The group selected specifies the destinations that the application user, such as IPMASysUser, can monitor.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP Dial Rules</td>
<td>If required, choose the appropriate SIP dial rule. SIP dial rules provide local dial plans for Cisco Unified IP Phones 7905, 7912, 7940, and 7960, so users do not have to press a key or wait for a timer before the call gets processed. Leave the SIP Dial Rules field set to <code>&lt;None&gt;</code> if you do not want dial rules to apply to the IP phone that is running SIP. This means that the user must use the Dial softkey or wait for the timer to expire before the call gets processed.</td>
</tr>
<tr>
<td>MTP Preferred Originating Codec</td>
<td>From the drop-down list box, choose the codec to use if a media termination point is required for SIP calls.</td>
</tr>
<tr>
<td>Device Security Profile</td>
<td>Choose the security profile to apply to the device.</td>
</tr>
<tr>
<td></td>
<td>You must apply a security profile to all phones that are configured in Cisco Unified Communications Manager Administration. Installing Cisco Unified Communications Manager provides a set of predefined, nonsecure security profiles for auto-registration. To enable security features for a phone, you must configure a new security profile for the device type and protocol and apply it to the phone. If the phone does not support security, choose a nonsecure profile. To identify the settings that the profile contains, choose System &gt; Security Profile &gt; Phone Security Profile.</td>
</tr>
<tr>
<td>Note</td>
<td>The CAPF settings that are configured in the profile relate to the Certificate Authority Proxy Function settings that display in the Phone Configuration window. You must configure CAPF settings for certificate operations that involve manufacturer-installed certificates (MICs) or locally significant certificates (LSC). See the Cisco Unified Communications Manager Security Guide for more information about how CAPF settings that you update in the phone configuration window affect security profile CAPF settings.</td>
</tr>
<tr>
<td>Rerouting Calling Search Space</td>
<td>From the drop-down list box, choose a calling search space to use for rerouting.</td>
</tr>
<tr>
<td></td>
<td>The rerouting calling search space of the referrer gets used to find the route to the refer-to target. When the Refer fails due to the rerouting calling search space, the Refer Primitive rejects the request with the “405 Method Not Allowed” message. The redirection (3xx) primitive and transfer feature also uses the rerouting calling search space to find the redirect-to or transfer-to target.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SUBSCRIBE Calling Search Space</td>
<td>Supported with the Presence feature, the SUBSCRIBE calling search space determines how Cisco Unified Communications Manager routes presence requests that come from the end user. This setting allows you to apply a calling search space separate from the call-processing search space for presence (SUBSCRIBE) requests for the end user. From the drop-down list box, choose the SUBSCRIBE calling search space to use for presence requests for the end user. All calling search spaces that you configure in Cisco Unified Communications Manager Administration display in the SUBSCRIBE Calling Search Space drop-down list box. If you do not select a different calling search space for the end user from the drop-down list, the SUBSCRIBE calling search space defaults to None. To configure a SUBSCRIBE calling search space specifically for this purpose, you configure a calling search space as you do all calling search spaces.</td>
</tr>
<tr>
<td>SIP Profile</td>
<td>Choose the default SIP profile or a specific profile that was previously created. SIP profiles provide specific SIP information for the phone such as registration and keepalive timers, media ports, and do not disturb control.</td>
</tr>
<tr>
<td>Digest User</td>
<td>Choose an end user that you want to associate with the phone for this setting that is used with digest authentication (SIP security). Ensure that you configured digest credentials for the user that you choose, as specified in the End User Configuration window. For more information on digest authentication, see the Cisco Unified Communications Manager Security Guide.</td>
</tr>
<tr>
<td>Media Termination Point Required</td>
<td>Use this field to indicate whether a media termination point is used to implement features that H.323 does not support (such as hold and transfer). Check the Media Termination Point Required check box if you want to use an MTP to implement features. Uncheck the Media Termination Point Required check box if you do not want to use an MTP to implement features. Use this check box only for H.323 clients and those H.323 devices that do not support the H.245 empty capabilities set or if you want media streaming to terminate through a single source. If you check this check box to require an MTP and this device becomes the endpoint of a video call, the call will be audio only.</td>
</tr>
<tr>
<td>Unattended Port</td>
<td>Check this check box to indicate an unattended port on this device.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Require DTMF Reception</td>
<td>For phones that are running SIP and SCCP, check this check box to require DTMF reception for this phone.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> In configuring Cisco Unified Mobility features, when using intercluster DNs as remote destinations for an IP phone via SIP trunk (either intercluster trunk [ICT] or gateway), check this check box so that DTMF digits can be received out of band, which is crucial for Enterprise Feature Access midcall features.</td>
</tr>
</tbody>
</table>

### Certification Authority Proxy Function (CAPF) Information

<table>
<thead>
<tr>
<th>Certificate Operation</th>
<th>From the drop-down list box, choose one of the following options:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• No Pending Operation—Displays when no certificate operation is occurring (default setting).</td>
</tr>
<tr>
<td></td>
<td>• Install/Upgrade—Installs a new or upgrades an existing locally significant certificate in the phone.</td>
</tr>
<tr>
<td></td>
<td>• Delete—Deletes the locally significant certificate that exists in the phone.</td>
</tr>
<tr>
<td></td>
<td>• Troubleshoot—Retrieves the locally significant certificate (LSC) or the manufacture installed certificate (MIC), so you can view the certificate credentials in the CAPF trace file. If both certificate types exist in the phone, Cisco Unified CM creates two trace files, one for each certificate type.</td>
</tr>
<tr>
<td></td>
<td>By choosing the Troubleshooting option, you can verify that an LSC or MIC exists in the phone.</td>
</tr>
<tr>
<td></td>
<td>For more information on CAPF operations, see the <em>Cisco Unified Communications Manager Security Guide</em>.</td>
</tr>
</tbody>
</table>
This field allows you to choose the authentication method that the phone uses during the CAPF certificate operation. From the drop-down list box, choose one of the following options:

- **By Authentication String**—Installs/upgrades, deletes, or troubleshoots a locally significant certificate only when the user enters the CAPF authentication string on the phone.

- **By Null String**— Installs/upgrades, deletes, or troubleshoots a locally significant certificate without user intervention. This option provides no security; Cisco strongly recommends that you choose this option only for closed, secure environments.

- **By Existing Certificate (Precedence to LSC)**—Installs/upgrades, deletes, or troubleshoots a locally significant certificate if a manufacture-installed certificate (MIC) or locally significant certificate (LSC) exists in the phone. If a LSC exists in the phone, authentication occurs via the LSC, regardless whether a MIC exists in the phone. If a MIC and LSC exist in the phone, authentication occurs via the LSC. If a LSC does not exist in the phone, but a MIC does exist, authentication occurs via the MIC. Before you choose this option, verify that a certificate exists in the phone. If you choose this option and no certificate exists in the phone, the operation fails.

  At any time, the phone uses only one certificate to authenticate to CAPF even though a MIC and LSC can exist in the phone at the same time. If the primary certificate, which takes precedence, becomes compromised for any reason, or, if you want to authenticate via the other certificate, you must update the authentication mode.

- **By Existing Certificate (Precedence to MIC)**—Installs, upgrades, deletes, or troubleshoots a locally significant certificate if a LSC or MIC exists in the phone. If a MIC exists in the phone, authentication occurs via the MIC, regardless whether a LSC exists in the phone. If a LSC exists in the phone, but a MIC does not exist, authentication occurs via the LSC. Before you choose this option, verify that a certificate exists in the phone. If you choose this option and no certificate exists in the phone, the operation fails.

**Note** The CAPF settings that are configured in the Phone Security Profile window interact with the CAPF parameters that are configured in the Phone Configuration window.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication String</td>
<td>If you chose the By Authentication String option in the Authentication Mode drop-down list box, this field applies. Manually enter a string or generate a string by clicking the <strong>Generate String</strong> button. Ensure that the string contains 4 to 10 digits. To install, upgrade, delete, or troubleshoot a locally significant certificate, the phone user or administrator must enter the authentication string on the phone.</td>
</tr>
<tr>
<td>Key Size (Bits)</td>
<td>For this setting that is used for CAPF, choose the key size for the certificate from the drop-down list box. The default setting equals 1024. Other options include 512 and 2048. If you choose a higher key size than the default setting, the phones take longer to generate the entropy that is required to generate the keys. Key generation, which is set at low priority, allows the phone to function while the action occurs. Depending on the phone model, you may notice that key generation takes up to 30 or more minutes to complete.</td>
</tr>
<tr>
<td>Note</td>
<td>The CAPF settings that are configured in the Phone Security Profile window interact with the CAPF parameters that are configured in the Phone Configuration window.</td>
</tr>
<tr>
<td>Operation Completes By</td>
<td>This field, which supports the Install/Upgrade, Delete, and Troubleshoot Certificate Operation options, specifies the date and time in which you must complete the operation. The values that display apply for the publisher database server.</td>
</tr>
<tr>
<td>Certificate Operation Status</td>
<td>This field displays the progress of the certificate operation; for example, <code>&lt;operation type&gt;</code> pending, failed, or successful, where operating type equals the Install/Upgrade, Delete, or Troubleshoot Certificate Operation options. You cannot change the information that displays in this field.</td>
</tr>
<tr>
<td>Enable Extension Mobility</td>
<td></td>
</tr>
<tr>
<td>Enable Extension Mobility</td>
<td>Check this check box if this phone supports extension mobility.</td>
</tr>
<tr>
<td>Log Out Profile</td>
<td>This drop-down list box specifies the device profile that the device uses when no one is logged in to the device by using Cisco Extension Mobility. You can choose either Use Current Device Settings or one of the specific configured profiles that are listed. If you select a specific configured profile, the system retains a mapping between the device and the login profile after the user logs out. If you select Use Current Device Settings, no mapping gets retained.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Log in Time</td>
<td>This field remains blank until a user logs in. When a user logs in to the device by using Cisco Extension Mobility, the time at which the user logged in displays in this field.</td>
</tr>
<tr>
<td>Log out Time</td>
<td>This field remains blank until a user logs in. When a user logs in to the device by using Cisco Extension Mobility, the time at which the system will log out the user displays in this field.</td>
</tr>
</tbody>
</table>

**MLPP Information**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MLPP Domain</td>
<td>Choose an MLPP domain from the drop-down list box for the MLPP domain that is associated with this device. If you leave the None value, this device inherits its MLPP domain from the value that was set for the device pool of the device. If the device pool does not have an MLPP domain setting, this device inherits its MLPP domain from the value that was set for the MLPP Domain Identifier enterprise parameter.</td>
</tr>
</tbody>
</table>

**Do Not Disturb**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do Not Disturb</td>
<td>Check this check box to enable Do Not Disturb on the remote device.</td>
</tr>
<tr>
<td>DND Option</td>
<td>When you enable DND on the phone, Ringer Off parameter turns off the ringer, but incoming call information gets presented to the device, so the user can accept the call.</td>
</tr>
</tbody>
</table>

**Product Specific Configuration Layout Information**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Video Capabilities | When enabled, indicates that the device will participate in video calls.  
Default: Enabled  |

You can view the directory numbers that are assigned to the phone from the Association Information area of the Phone Configuration window. After you add a phone, the Association Information area displays on the left side of the Phone Configuration window.
Table 44: Association Information Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Modify Button Items</td>
<td>After you add a phone, the Association Information area displays on the left side of the Phone Configuration window. Click this button to manage button associations for this phone. A dialog box warns that any unsaved changes to the phone may be lost. If you have saved any changes that you made to the phone, click OK to continue. The Reorder Phone Button Configuration window displays for this phone. See the Modifying Phone Button Template Button Items topic for a detailed procedure.</td>
</tr>
<tr>
<td>Line [1] - Add a new DN Line [2] - Add a new DN</td>
<td>After you add a phone, the Association Information area displays on the left side of the Phone Configuration window. Click these links to add a directory number(s) that associates with this phone. When you click one of the links, the Directory Number Configuration window displays. See the Directory Number Configuration Settings section for details.</td>
</tr>
</tbody>
</table>

Cisco IP Communicator

Cisco IP Communicator, a software-based application, allows users to place and receive phone calls by using their personal computers. Cisco IP Communicator depends upon the Cisco Unified Communications Manager call-processing system to provide telephony features and voice-over-IP capabilities.

This interaction with Cisco Unified Communications Manager means that Cisco IP Communicator provides the same functionality as a full-featured Cisco Unified IP Phone, while providing the portability of a desktop application. Additionally, it means that you administer Cisco IP Communicator as a phone device by using the Cisco Unified Communications Manager Administration Phone Configuration window.

Cisco Unified Personal Communicator

Cisco Unified Personal Communicator, a desktop software application, provides access to voice, video, document-sharing, and presence applications - all from a single, rich media interface. Cisco Unified Personal Communicator relies on the Cisco Unified Communications Manager call-processing system to provide telephony features and voice-over-IP capabilities.

This interaction with Cisco Unified Communications Manager enables Cisco Unified Personal Communicator to offer integrated softphone capabilities and control of the physical IP phone of the user. Additionally, it
means you administer Cisco Unified Personal Communicator as a phone device by using the Cisco Unified Communications Manager Administration Phone Configuration window.

Cisco TelePresence

The Cisco TelePresence Meeting Solution, a visual meeting room solution that comprises endpoints, IP telephony infrastructure technology, and user software applications, enables life-size, “you are there” video teleconferencing. The Cisco TelePresence IP Phone represents an integral part of the solution that provides the user interface for making connections to other Cisco TelePresence meeting rooms and for driving the codec, the device that manages the plasma display screens, microphones, speakers, and cameras that create the virtual meeting experience. The Cisco TelePresence IP Phone offers both standard Cisco Unified IP Phone 7975 and Cisco TelePresence meeting connection functionality. As an example, the Cisco TelePresence IP Phone user interface displays a schedule of the meetings for the day and provides softkeys that are designed to enable and enhance the teleconference connections but then can be used during the video teleconference to add audio meeting participants or to make voice calls.

For more information about Cisco TelePresence, see the following system and configuration documentation:

- Cisco TelePresence System Administrators Guide
- Cisco TelePresence Meeting User’s Guide
- Cisco Unified Communications Manager and Cisco TelePresence Configuration

Cisco Unified Mobile Communicator

Cisco Unified Mobile Communicator specifies a software application for mobile handsets that extends enterprise communications applications and services to mobile phones and smartphones. Cisco Unified Mobile Communicator streamlines the communication experience, enabling real-time collaboration across the enterprise.

To configure a Cisco Unified Mobile Communicator, choose the Device > Phone menu option in Cisco Unified Communications Manager Administration.

Codec usage

Cisco Unified Communications Manager supports the Advertise G.722 Codec enterprise parameter, which determines whether Cisco Unified IP Phones advertise the G.722 codec to Cisco Unified Communications Manager. Codec negotiation involves two steps. First, the phone must advertise the supported codec(s) to Cisco Unified Communications Manager (not all phones support the same set of codecs). Second, when Cisco Unified Communications Manager gets the list of supported codecs from all phones that are involved in the call attempt, it chooses a commonly supported codec based on various factors, including the region pair setting. Valid values specify True (the specified Cisco Unified IP Phones advertise G.722 to Cisco Unified Communications Manager) or False (the specified Cisco Unified IP Phones do not advertise G.722 to Cisco Unified Communications Manager).

Note

The default for the Advertise G.722 Codec enterprise parameter enables G.722 on all phones in the cluster. The default value of the phone configuration Advertise G.722 Codec Product-Specific parameter uses the value that the enterprise parameter setting specifies.
The Product Specific Configuration Layout area in the Phone Configuration window supports the parameter, Advertise G.722 Codec. Use this parameter to override the enterprise parameter on an individual phone basis.

The following table indicates how the phone responds to the configuration options.

Table 45: How Phone Responds to Configuration Settings

<table>
<thead>
<tr>
<th>Enterprise Parameter Setting</th>
<th>Phone (Product-Specific) Parameter Setting</th>
<th>Phone Advertises G.722</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advertise G.722 Codec Enabled</td>
<td>Use System Default</td>
<td>Yes</td>
</tr>
<tr>
<td>Advertise G.722 Codec Enabled</td>
<td>Enabled</td>
<td>Yes</td>
</tr>
<tr>
<td>Advertise G.722 Codec Enabled</td>
<td>Disabled</td>
<td>No</td>
</tr>
<tr>
<td>Advertise G.722 Codec Disabled</td>
<td>Use System Default</td>
<td>No</td>
</tr>
<tr>
<td>Advertise G.722 Codec Disabled</td>
<td>Enabled</td>
<td>Yes</td>
</tr>
<tr>
<td>Advertise G.722 Codec Disabled</td>
<td>Disabled</td>
<td>No</td>
</tr>
</tbody>
</table>

Cisco Unified Communications Manager supports G.722, which is a wideband codec, as well as a propriety codec simply named Wideband. Both represent wideband codecs. Wideband codecs such as G.722 provide a superior voice experience because wideband frequency response is 200 Hz to 7 kHz compared to narrowband frequency response of 300 Hz to 3.4 kHz. At 64 kb/s, the G.722 codec offers conferencing performance and good music quality.

When users use a headset that supports wideband, they experience improved audio sensitivity when the wideband setting on their phones is enabled (it is disabled by default). To access the wideband headset setting on the phone, users choose the Settings icon User Preferences > Audio Preferences > Wideband Headset. Users should check with their system administrator to be sure their phone system is configured to use G.722 or wideband. If the system is not configured for a wideband codec, they may not detect any additional audio sensitivity, even when they are using a wideband headset.

The following Cisco Unified IP Phones (both SCCP and SIP) support the wideband codec G.722 for use with a wideband headset:

- Cisco Unified IP Phone 7906G
- Cisco Unified IP Phone 7911G
- Cisco Unified IP Phone 7931G
- Cisco Unified IP Phone 7942G
- Cisco Unified IP Phone 7945G
- Cisco Unified IP Phone 7962G
- Cisco Unified IP Phone 7965G
- Cisco Unified IP Phone 7975G
- Cisco Unified IP Phone 8961
When you choose a G.711 or G.722 codec in Region Configuration, you are choosing the bandwidth utilization. Choosing either codec produces the same affect. When you choose either G.711 or G.722, these codecs disallow selecting codecs that have a payload greater than 64 kb/s, such as the G.722 wideband codec and Advanced Audio Codec (AAC) (when AAC uses more than one channel).

If you choose a region that is lower than G.711 or G.722, the Advertise G.722 Codec enterprise parameter gets ignored because the system does not allow G.722, G.711, AAC, and wideband.

Tip
Enabling the Advertise G.722 Codec parameter causes interoperability problems with call park and ad hoc conferences. When you use the enterprise parameter with features such as ad hoc conferencing and call park, change the setting to Disabled and update the device pools for the phones.

When enabled, the service parameter allows Cisco Unified IP Phones (such as 7971, 7970, 7941, 7961) to negotiate and use the G.722 codec when calls are within the same region.

If individual phone control and use of a specific codec type is required (for example, G.711), check the configuration of each phone (by using Phone Configuration) for the parameter Advertise G.722 Codec, and change the setting to Disabled. Save and reset the device.

Note
If the Advertise G.722 Codec enterprise parameter is set to Enabled, the administrator can override this by using the G.722 Codec Enabled service parameter. This service parameter determines whether Cisco Unified Communications Manager supports G.722 negotiation for none, some, or all devices. Valid values specify Enabled for All Devices (support G.722 for all devices), Enabled for All Devices Except Recording-Enabled Devices (support G.722 for all devices except those that have call recording enabled), or Disabled (do not support G.722 codec).

Phone button templates
Cisco Unified Communications Manager includes several default phone button templates. When adding phones, you can assign one of these templates to the phones or create a new template.
Creating and using templates provide a fast way to assign a common button configuration to a large number of phones. For example, if users in your company do not use the conference feature, you can create a template that reassigns this button to a different feature, such as speed dial.
To create a template, you must make a copy of an existing template and assign the template a unique name. You can make changes to the custom templates that you created, and you can change the labels of the default phone button templates. You cannot change the function of the buttons in the default templates. You can rename existing templates and modify them to create new ones, update custom templates to add or remove features, lines, or speed dials, and delete custom templates that are no longer being used. When you update a template, the change affects all phones that use the template.
Renaming a template does not affect the phones that use that template. All Cisco Unified IP Phones that use this template continue to use this template after it is renamed.
Make sure that all phones have at least one line that is assigned to each phone. Normally, this assignment specifies button 1. Phones can have additional lines that are assigned, depending on the Cisco Unified IP
Phone model. Phones also generally have several features, such as speed dial, that are assigned to the remaining buttons.

You can delete phone templates that are not currently assigned to any phone in your system if they are not the only template for a given phone model. You cannot delete a template that is assigned to one or more devices or the default template for a model (specified in the Device Defaults Configuration window). You must reassign all Cisco Unified IP Phones that are using the template that you want to delete to a different phone button template before you can delete the template.

Note

Use a copy of the standard phone button template for button assignment. The standard phone button template for any phone that supports expansion module include buttons for both the phone and the expansion module. For example, the Cisco Unified IP Phone 7965, which supports the Cisco Unified IP Phone Expansion Module 7915, includes buttons for both devices (up to 48 buttons).

Choose Dependency Records from the Related Links drop-down list box on the Phone Button Template Configuration window to view the devices that are using a particular template.

Cisco Unified Communications Manager does not directly control all features on Cisco Unified IP Phones through phone button templates. See the Cisco Unified IP Phone Administration Guide for Cisco Unified Communications Manager and other phone documentation for detailed information about individual Cisco Unified IP Phone family models.

Default phone button templates

Although all Cisco Unified IP Phones support similar features, you implement these features differently on various models. For example, some models configure features such as Hold or Transfer by using phone button templates; other models have fixed buttons or onscreen program keys for these features that are not configurable. Also, the maximum number of lines or speed dials that are supported differs for some phone models. These differences require different phone button templates for specific models.

Each Cisco Unified IP Phone comes with a default phone button template. You can use the default templates as is to quickly configure phones. You can also copy and modify the templates to create custom templates.

Custom templates enable you to make features available on some or all phones, restrict the use of certain features to certain phones, configure a different number of lines or speed dials for some or all phones, and so on, depending on how the phone will be used. For example, you may want to create a custom template that can be applied to phones that will be used in conference rooms.

The following table provides descriptions of the standard phone button templates.

Table 46: Default Phone Button Templates Listed by Model

<table>
<thead>
<tr>
<th>Phone Button Template Name</th>
<th>Template Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Phone Button Template Name</td>
<td>Template Description</td>
</tr>
<tr>
<td>----------------------------</td>
<td>----------------------</td>
</tr>
<tr>
<td>Standard 7985</td>
<td>The Standard 7985 template uses buttons 1 and 2 for lines and assigns buttons 3 through 8 as speed dials. Access other phone features, such as call park, call forward, redial, hold, resume, voice-messaging system, conferencing, and so on, by using softkeys on the Cisco IP Video Phone 7985.</td>
</tr>
<tr>
<td>Standard 7971 SCCP</td>
<td>The Standard 7971 SCCP template uses buttons 1 and 2 for lines and assigns buttons 3 through 8 as speed dials. Access other phone features, such as call park, call forward, redial, hold, resume, voice-messaging system, conferencing, and so on, by using softkeys on the Cisco Unified IP Phone 7971.</td>
</tr>
<tr>
<td>Standard 7971 SIP</td>
<td>The Standard 7971 SIP template uses buttons 1 and 2 for lines and assigns buttons 3 through 8 as speed dials. Access other phone features, such as call park, call forward, redial, hold, resume, voice-messaging system, conferencing, and so on, by using softkeys on the Cisco Unified IP Phone 7971.</td>
</tr>
<tr>
<td>Standard 7970 SCCP</td>
<td>The Standard 7970 SCCP template uses buttons 1 and 2 for lines and assigns buttons 3 through 8 as speed dials. Access other phone features, such as call park, call forward, redial, hold, resume, voice-messaging system, conferencing, and so on, by using softkeys on the Cisco Unified IP Phone 7970.</td>
</tr>
<tr>
<td>Standard 7970 SIP</td>
<td>The Standard 7970 SIP template uses buttons 1 and 2 for lines and assigns buttons 3 through 8 as speed dials. Access other phone features, such as call park, call forward, redial, hold, resume, voice-messaging system, conferencing, and so on, by using softkeys on the Cisco Unified IP Phone 7970.</td>
</tr>
<tr>
<td>Standard 7961 SCCP and Standard 7961G-GE SCCP</td>
<td>The Standard 7961 SCCP template uses buttons 1 and 2 for lines and assigns buttons 3 through 6 as speed dials or lines or for the features privacy and service URL. Access other phone features, such as abbreviated dial, call park, call forward, redial, hold, resume, call back, conferencing, and so on, by using softkeys on the Cisco Unified IP Phone 7961.</td>
</tr>
<tr>
<td>Standard 7961 SIP</td>
<td>The Standard 7961 SIP template uses buttons 1 and 2 for lines and assigns buttons 3 through 6 as speed dials or lines or for the features privacy and service URL. Access other phone features, such as abbreviated dial, call park, call forward, redial, hold, resume, call back, conferencing, and so on, by using softkeys on the Cisco Unified IP Phone 7961.</td>
</tr>
<tr>
<td>Phone Button Template Name</td>
<td>Template Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>----------------------</td>
</tr>
<tr>
<td>Standard 7960 SCCP and Standard 7960 SIP</td>
<td>The Standard 7960 SCCP and SIP templates use buttons 1 and 2 for lines and assigns buttons 3 through 6 as speed dials or lines or for the features privacy and service URL. Access other phone features, such as abbreviated dial, call park, call forward, redial, hold, resume, call back, conferencing, and so on, by using softkeys on the Cisco Unified IP Phone 7960.</td>
</tr>
<tr>
<td>Standard 7960 SIP</td>
<td>The Standard 7960 SIP template uses buttons 1 and 2 for lines and assigns buttons 3 through 6 as speed dials or lines or for the features privacy and service URL. Access other phone features, such as abbreviated dial, call park, call forward, redial, hold, resume, call back, conferencing, and so on, by using softkeys on the Cisco Unified IP Phone 7960.</td>
</tr>
<tr>
<td>Standard 7941 SCCP and Standard 7941G-GE SCCP</td>
<td>The Standard 7941 SCCP template comes with a preconfigured one-line phone button template (button 1 for line 1 and button 2 for speed dial). Access phone features, such as abbreviated dial, call park, call forward, redial, hold, resume, call back, conferencing, and so on, by using softkeys on the Cisco Unified IP Phone 7941.</td>
</tr>
<tr>
<td>Standard 7941 SIP</td>
<td>The Standard 7940 SIP template comes with a preconfigured one-line phone button template (button 1 for line 1 and button 2 for speed dial). Access phone features, such as abbreviated dial, call park, call forward, redial, hold, resume, call back, conferencing, and so on, by using softkeys on the Cisco Unified IP Phone 7941.</td>
</tr>
<tr>
<td>Standard 7940 SCCP and Standard 7940 SIP</td>
<td>The Standard 7940 SCCP templates comes with a preconfigured one-line phone button template (button 1 for line 1 and button 2 for speed dial). Access phone features, such as abbreviated dial, call park, call forward, redial, hold, resume, call back, conferencing, and so on, by using softkeys on the Cisco Unified IP Phone 7940.</td>
</tr>
<tr>
<td>Standard 7940 SIP</td>
<td>The Standard 7940 SIP template comes with a preconfigured one-line phone button template (button 1 for line 1 and button 2 for speed dial). Access phone features, such as abbreviated dial, call park, call forward, redial, hold, resume, call back, conferencing, and so on, by using softkeys on the Cisco Unified IP Phone 7940.</td>
</tr>
<tr>
<td>Standard 7931 SCCP and Standard 7931 SIP</td>
<td>The Standard 7931 SCCP and SIP templates use button 1 for line 1.</td>
</tr>
<tr>
<td>Standard 7920</td>
<td>The Standard 7920 template uses buttons 1 and 2 for lines and assigns buttons 3 through 6 for speed dials.</td>
</tr>
<tr>
<td>Phone Button Template Name</td>
<td>Template Description</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Standard 7912 SCCP</td>
<td>The Standard 7912 SCCP template uses button 1 for line 1, buttons 2 through 5 for speed dial, button 6 for Hold, and button 7 for Settings.</td>
</tr>
<tr>
<td>Standard 7912 SIP</td>
<td>The Standard 7912 SIP template uses button 1 for line 1, buttons 2 through 5 for speed dial, button 6 for Hold, and button 7 for Settings.</td>
</tr>
<tr>
<td>Standard 7911 SCCP and Standard 7911 SIP</td>
<td>The Standard 7911 SCCP and SIP templates use button 1 for line 1, makes button 2 configurable as the Privacy softkey (default specifies None), and assigns buttons 3 through 6 as speed dials. The user accesses speed dials from the Directories menu or the Navigation button on the phone.</td>
</tr>
<tr>
<td>Standard 7911 SIP</td>
<td>The Standard 7911 SIP template uses button 1 for line 1, makes button 2 configurable as the Privacy softkey (default specifies None), and assigns buttons 3 through 6 as speed dials. The user accesses speed dials from the Directories menu or the Navigation button on the phone.</td>
</tr>
</tbody>
</table>
| Standard 7910              | The Standard 7910 template uses button 1 for message waiting, button 2 for conference, button 3 for forwarding, buttons 4 and 5 for speed dial, and button 6 for redial. 
The Cisco Unified IP Phone 7910 includes fixed buttons for Line, Hold, Transfer, and Settings. |
<p>| Standard 7906 SCCP and Standard 7906 SIP | The Standard 7906 SCCP and SIP templates use button 1 for line 1, makes button 2 configurable as the Privacy softkey (default specifies None), and assigns buttons 3 through 6 as speed dials. The user accesses speed dials from the Directories menu or the Navigation button on the phone. |
| Standard 7906 SIP          | The Standard 7906 SIP template uses button 1 for line 1, makes button 2 configurable as the Privacy softkey (default specifies None), and assigns buttons 3 through 6 as speed dials. The user accesses speed dials from the Directories menu or the Navigation button on the phone. |
| Standard 7905 SCCP         | The Standard 7905 SCCP template uses button 1 for line 1, buttons 2 through 5 for speed dial, button 6 for Hold, and button 7 for Settings.           |
| Standard 7905 SIP          | The Standard 7905 SIP template uses button 1 for line 1, buttons 2 through 5 for speed dial, button 6 for Hold, and button 7 for Settings.            |
| Standard 7902              | The Standard 7902 template uses button 1 for line 1, buttons 2 through 5 for speed dial, button 6 for Hold, and button 7 for Settings.             |
| Standard 7936              | The Standard 7936 template, which is not configurable for the Cisco Unified IP Conference Station 7936, uses button 1 for line 1.                   |</p>
<table>
<thead>
<tr>
<th>Phone Button Template Name</th>
<th>Template Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard 7935</td>
<td>The Standard 7935 template, which is not configurable for the Cisco IP Conference Station 7935, uses button 1 for line 1.</td>
</tr>
</tbody>
</table>
| Standard 30 SP+          | The Standard 30 SP+ template uses buttons 1 through 4 for lines, button 5 for call park, buttons 6 through 8 and 17 through 21 remain undefined, and buttons 9 through 13 and 22 through 25 apply for speed dial; button 14 applies for message-waiting indicator, button 15 for forward, and button 16 for conference.  
**Note** For only the Cisco IP Phone 30 SP+, assign button 26 for automatic echo cancellation (AEC). |
<p>| Standard 30 VIP          | The Standard 30 VIP template uses buttons 1 through 4 for lines, button 5 for call park, buttons 6 through 13 and 22 through 26 for speed dial, button 14 for message-waiting indicator, button 15 for call forward, and button 16 for conference. |
| Standard 12 Series, including the 12 S, 12 SP, and 12 SP+ | The Standard 12 S, Standard 12 SP, and Standard 12 SP+ templates use buttons 1 and 2 for lines, button 3 for redial, buttons 4 through 6 for speed dial, button 7 for hold, button 8 for transfer, button 9 for forwarding, button 10 for call park, button 11 for message waiting, and button 12 for conference. |
| Default VGC Virtual Phone | The Default VGC Virtual Phone template for the Cisco VGC Virtual Phone uses button 1 for line 1. |
| Standard Analog          | The Standard Analog template for analog phones uses button 1 for line 1. |
| Standard ATA 186         | The Standard ATA 186 template for the Cisco ATA 186 Analog Telephone Adaptor uses button 1 for a line and buttons 2 through 10 for speed dials. |
| ISDN BRI Phone           | The ISDN BRI Phone template uses button 1 for line 1. |
| Standard CIPC SCCP       | The Standard CIPC (Cisco IP Communicator) SCCP template uses buttons 1 and 2 for lines and assigns buttons 3 through 8 as speed dials. Access other phone features, such as call park, call forward, redial, hold, resume, voice-messaging system, conferencing, and so on, by using softkeys (by configuring the softkey template to the phone). |</p>
<table>
<thead>
<tr>
<th>Phone Button Template Name</th>
<th>Template Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard CIPC SIP</td>
<td>The Standard CIPC SIP template uses buttons 1 and 2 for lines and assigns buttons 3 through 8 as speed dials. Access other phone features, such as call park, call forward, redial, hold, resume, voice-messaging system, conferencing, and so on, by using softkeys (by configuring the softkey template to the phone).</td>
</tr>
<tr>
<td>Standard IP-STE</td>
<td>The Standard IP-STE template uses buttons 1 and 2 for lines.</td>
</tr>
<tr>
<td>Standard Unified Communicator SIP</td>
<td>The Standard Unified Communicator SIP template uses button 1 for line 1.</td>
</tr>
<tr>
<td>Standard VGC Phone</td>
<td>The Standard VGC Phone template for the Cisco VG248 Gateway uses button 1 for a line and buttons 2 through 10 for speed dials.</td>
</tr>
<tr>
<td>Standard Cisco TelePresence</td>
<td>The Standard Cisco TelePresence template, required by Cisco TelePresence, uses buttons 1 and 2 for lines and buttons 3 through 42 for speed dials.</td>
</tr>
<tr>
<td>Third-Party SIP Device (Advanced)</td>
<td>The Generic SIP Phone - 2 Lines template, which is used for third-party phones that run SIP, uses buttons 1 and 2 for lines.</td>
</tr>
<tr>
<td>Third-Party SIP Device (Basic)</td>
<td>The Generic SIP Phone - 2 Lines template, which is used for third-party phones that run SIP, uses buttons 1 and 2 for lines.</td>
</tr>
<tr>
<td>Third-Party AS-SIP Device</td>
<td>The Generic SIP Phone - 2 Lines template, which is used for third-party phones that run SIP, uses buttons 1 and 2 for lines.</td>
</tr>
</tbody>
</table>

**Guidelines for customizing phone button templates**

Use the following guidelines when you are creating custom phone button templates:

- Make sure that phone users receive a quick reference card or getting started guide that describes the most basic features of the custom template. If you create a custom template for employees in your company to use, make sure that it includes the following features and that you describe them on the quick reference card that you create for your users:
Consider the nature of each feature to determine how to configure your phone button template. You may want to assign multiple buttons to speed dial and line; however, you usually require only one of the other phone button features that are described in Table 36-6.

**Table 47: Phone Button Feature Description**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AEC</td>
<td>If you are configuring a template for the Cisco IP Phone 30 VIP, you must include one occurrence of this feature and assign it to button 26. Auto echo cancellation (AEC) reduces the amount of feedback that the called party receives when the calling party is using a speakerphone. Users should press the AEC button on a Cisco IP Phone 30 SP+ when they are using speakerphone. Users do not need to press this button when speakerphone is not in use. This feature requires no configuration for it to work.</td>
</tr>
<tr>
<td>Answer/release</td>
<td>In conjunction with a headset apparatus, the user can press a button on the headset apparatus to answer and release (disconnect) calls.</td>
</tr>
<tr>
<td>Auto answer</td>
<td>If this feature is programmed on the template, pressing this button causes the speakerphone to go off hook automatically when an incoming call is received.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> You configure this feature for some phones models by using the Phone Button Template window, and you configure this feature for some phone models by using the Phone Configuration window.</td>
</tr>
<tr>
<td>Call park</td>
<td>In conjunction with a call park number or range, when the user presses this button, call park places the call at a directory number for later retrieval. You must have a call park number or range that is configured in the system for this button to work, and you should provide that number or range to your users, so they can dial in to the number(s) to retrieve calls.</td>
</tr>
</tbody>
</table>
## Table: Phone button templates

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
</table>
| Call Park BLF  | Users can monitor the busy/idle status of directed call park numbers using the Call Park Busy Lamp Field (BLF) buttons. Users can also speed dial those numbers by pressing the BLF buttons. One directed call park number gets configured for each Call Park BLF button. To successfully park or retrieve a call by using a Call Park BLF button, you must ensure that the partition and the calling search space of the device are configured correctly.  
**Note** Use this button with the directed call park feature (a transfer function), not with the standard call park feature (a hold function). |
| Conference     | Users can initiate an ad hoc conference and add participants by pressing the Conference button. (Users can also use the Join softkey to initiate an ad hoc conference.)  
Only the person who initiates an ad hoc conference needs a conference button. You must make sure that an ad hoc conference bridge device is configured in Cisco Unified Communications Manager Administration for this button to work. See the Conference bridges, on page 265 chapter for more information. |
<p>| Forward all    | Users press this button to forward all calls to the designated directory number. Users can designate forward all in the Cisco Unified IP Phone Configuration windows, or you can designate a forward all number for each user in Cisco Unified Communications Manager Administration. |
| Hold           | Users press this button to place an active call on hold. To retrieve a call on hold, users press the flashing line button or lift the handset and press the flashing line button for the call on hold. The caller on hold receives a tone every 10 seconds to indicate the hold status or music (if the Music On Hold feature is configured). The hold tone feature requires no configuration to work. |
| Line           | Users press this button to dial a number or to answer an incoming call. For this button to work, you must have added directory numbers on the user phone. |</p>
<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Meet-Me conference</td>
<td>When users press this button, they initiate a meet-me conference, and they expect other invited users to dial in to the conference. Only the person who initiates a meet-me conference needs a meet-me button. You must ensure that a meet-me conference device is configured in Cisco Unified Communications Manager Administration for this button to work.</td>
</tr>
<tr>
<td>Message waiting</td>
<td>Users press this button to connect to the voice-messaging system.</td>
</tr>
<tr>
<td>None</td>
<td>Use None to leave a button unassigned.</td>
</tr>
<tr>
<td>Privacy</td>
<td>Users press this button to activate/deactivate privacy.</td>
</tr>
<tr>
<td>Redial</td>
<td>Users press this button to redial the last number that was dialed on the Cisco Unified IP Phone. This feature requires no configuration to work.</td>
</tr>
<tr>
<td>Service URL</td>
<td>Users press this button to access a Cisco Unified IP Phone Service such as personal fast dials, stock quotes, or weather.</td>
</tr>
<tr>
<td>Speed Dial</td>
<td>Users press this button to speed dial a specified number. System administrators can designate speed-dial numbers in Cisco Unified Communications Manager Administration. Users can designate speed-dial numbers in the Cisco Unified CM User Options menu.</td>
</tr>
<tr>
<td>Speed Dial/BLF</td>
<td>Users monitor this button for the real-time status of the associated directory number or SIP URI on those devices that support the presence feature. Users press this button to dial the destination.</td>
</tr>
<tr>
<td>Transfer</td>
<td>Users press this button to transfer an active call to another directory number. This feature requires no configuration to work.</td>
</tr>
</tbody>
</table>

**Programmable line keys**

Cisco Unified IP Phones support line buttons (the buttons next to the phone screen), which are used to initiate, answer, or switch to a call on a particular line. A limited number of features, such as speed dial, extension mobility, privacy, BLF speed dial, DND, and Service URLs, get assigned to these buttons.
The Programmable Line Key (PLK) feature expands the list of features that can be assigned to the line buttons to include features that softkeys normally control; for example, New Call, Call Back, End Call, and Forward All. When you configure these features on the line buttons, they always remain visible, so you can have a “hard” New Call key.

Programmable line keys support up to 27 features on line buttons (see Table 36-6). Use the Phone Button Template Configuration window to assign programmable line keys. It provides the appropriate configurable feature for the phone model. After configuring the phone button template, you must assign the phone button template to the phone by using Phone Configuration (reset is required).

Table 48: Programmable Line Keys for Cisco Unified IP Phones

<table>
<thead>
<tr>
<th>Feature</th>
<th>Phone Model 7971, 7970, 7961, 7941, 7914, 7915, 7916</th>
<th>Phone Model 7931 (SCCP only)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Redial</td>
<td>Yes</td>
<td>No, uses existing line button</td>
</tr>
<tr>
<td>Hold</td>
<td>Yes</td>
<td>No, uses existing line button</td>
</tr>
<tr>
<td>Transfer</td>
<td>Yes</td>
<td>No, uses existing line button</td>
</tr>
<tr>
<td>Privacy</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Forward All</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Meet Me</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Conference</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Park</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Pickup</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Group Call Pickup</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Malicious Caller ID (MCID)</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Conf List</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Remove Last Participant</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>QRT</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Call Back</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Other Call Pickup</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Video Mode</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>New Call</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>End Call</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Feature</td>
<td>Phone Model 7971, 7970, 7961, 7941, 7914, 7915, 7916</td>
<td>Phone Model 7931 (SCCP only)</td>
</tr>
<tr>
<td>--------------------</td>
<td>---------------------------------------------------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td>HLog (Hunt Group)</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Mobility</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Settings</td>
<td>No, uses existing button</td>
<td>Yes</td>
</tr>
<tr>
<td>Information</td>
<td>No, uses existing button</td>
<td>No</td>
</tr>
<tr>
<td>Services</td>
<td>No, uses existing button</td>
<td>Yes</td>
</tr>
<tr>
<td>Messages</td>
<td>No, uses existing button</td>
<td>Yes</td>
</tr>
<tr>
<td>Directories</td>
<td>No, uses existing button</td>
<td>Yes</td>
</tr>
<tr>
<td>AppMenu</td>
<td>No, uses existing button</td>
<td>Yes</td>
</tr>
<tr>
<td>Headset</td>
<td>No, uses existing button</td>
<td>Yes</td>
</tr>
</tbody>
</table>

The programmable line feature does not affect the existing softkey functionality. Softkeys still display as required and will continue to be specific to the state of the phone (for example, making a call, being in a call, navigating the Services menu).

If a feature is already assigned to a programmable line key, it can also appear as a softkey (and vice versa).

If a phone has a hard button for a feature, it cannot also have that feature as a programmable line key; for example, transfer cannot be a programmable line key on a Cisco Unified IP Phone 7931 because it already has a dedicated hard transfer button.

**Softkey templates**

Use softkey templates to manage softkeys that are associated with applications such as Cisco Unified Communications Manager Assistant or call-processing features such as Call Back on Cisco Unified IP Phones. You access the Softkey Template Configuration windows in Cisco Unified Communications Manager Administration to create and update softkey templates. (Device > Device Settings > Softkey Templates)

Cisco Unified Communications Manager supports two types of softkey templates: standard and nonstandard. Standard softkey templates in the Cisco Unified Communications Manager database contain the recommended selection and positioning of the softkeys for an application. Cisco Unified Communications Manager provides the following standard softkey templates:

- Standard User
- Standard Chaperone Phone
- Standard Feature
- Standard Assistant
- Standard Protected Phone
For most Cisco Unified IP Phone models, such as the Cisco Unified IP Phone 7945, 7965, 7975, and so on, you must assign standard or nonstandard softkey templates to the Cisco Unified IP Phone by assigning the templates individually to each phone or by assigning the common device configuration to each phone. Some Cisco Unified IP Phone models, such as the Cisco Unified IP Phone 8961, 9971, and 9951, do not use softkey templates. To determine whether your phone uses softkey templates and to determine which softkeys are supported on your phone, see the Cisco Unified IP Phone Phone Guide for your phone model.

You create a nonstandard softkey template by using the Softkey Template Configuration windows in Cisco Unified Communications Manager Administration. To create a nonstandard softkey template, the administrator copies a standard softkey template and makes changes. The administrator can add and remove applications that are associated with any nonstandard softkey template. Additionally, the administrator can configure softkey sets for each call state for a nonstandard softkey template.

The Softkey Template Configuration window lists the standard and nonstandard softkey templates and uses different icons to differentiate between standard and nonstandard templates.

The administrator assigns softkey templates in the following Cisco Unified Communications Manager Administration configuration windows:

- Common Device Configuration
- Phone Configuration (SIP and SCCP)
- UDP Template Configuration
- Default Device Profile Configuration

Add application

You can add a standard softkey template that is associated with a Cisco application to a nonstandard softkey template. When the administrator clicks the **Add Application** button from the Softkey Template Configuration window, a separate window displays and allows you to choose the standard softkey template that is to be added to the end of the nonstandard softkey template. Duplicate softkeys get deleted from the end of the set that is moving to the front of the set.

To refresh the softkeys for an application in the nonstandard softkey template, choose the standard softkey template that is already associated with the nonstandard softkey template. For example, if the administrator originally copied the Standard User template and deleted some buttons, choose the Standard User softkey template by clicking on the **Add Application** button. This adds the buttons that are included in the chosen softkey template.

The number of softkeys in any given call state cannot exceed 16. A message displays, and the add application procedure stops when the maximum number of softkeys is reached. The administrator must manually remove some softkeys from the call state before trying to add another application to the template.

The **Remove Application** button allows you to delete application softkey templates that are associated with a nonstandard softkey template. Only the softkeys that are associated with the application get deleted.
softkeys are commonly shared between applications, they remain in the softkey template until the last application that shares the softkeys is removed from the softkey template.

**Configure softkey layout**

The administrator can configure softkey sets for each call state for a nonstandard softkey template. When the administrator chooses Configure Softkey Layout from the Related Links drop-down list box on the Softkey Template Configuration window and clicks Go, the Softkey Layout Configuration window displays.

The Softkey Layout Configuration window allows you to specify the softkeys and their relative order for any phone models that support downloadable softkey templates. This window lists all softkeys, even though some phone models do not support all softkeys. To determine whether your phone model supports a softkey, see the Cisco Unified IP Phone Phone Guide for your phone model. If you choose a softkey that is not supported by the phone, the softkey does not display on the phone, even if you add it to the Selected Softkeys pane.

---

**Note**

Cisco recommends that a softkey remain in the same position for each call state. This provides the user with consistency and ease of use; for example, the More softkey always appears in the fourth softkey position from the left for each call state.

The Softkey Layout Configuration pane contains the following fields:

- Select a call state to configure-This drop-down list box displays the different call states of a Cisco Unified IP Phone. You cannot add, update, or delete call states. The call state that gets chosen from the drop-down list box indicates the softkeys that are available for that call state. Table 36-8 lists the call states.

<table>
<thead>
<tr>
<th>Call State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connected</td>
<td>Displays when call is connected</td>
</tr>
<tr>
<td>Connected Conference</td>
<td>Consultation call for conference in connected call state</td>
</tr>
<tr>
<td>Connected Transfer</td>
<td>Consultation call for transfer in connected call state</td>
</tr>
<tr>
<td>Digits After First</td>
<td>Off-hook call state after user enters the first digit</td>
</tr>
<tr>
<td>Off Hook</td>
<td>Dial tone presented to phone</td>
</tr>
<tr>
<td>Off Hook With Feature</td>
<td>Off-hook call state for transfer or conference consultation call</td>
</tr>
<tr>
<td>On Hold</td>
<td>Call on hold</td>
</tr>
<tr>
<td>On Hook</td>
<td>No call exists for that phone.</td>
</tr>
<tr>
<td>Remote In Use</td>
<td>Another device that shares the same line uses call.</td>
</tr>
<tr>
<td>Ring In</td>
<td>Call received and ringing</td>
</tr>
<tr>
<td>Ring Out</td>
<td>Call initiated and the destination ringing</td>
</tr>
</tbody>
</table>
• **Unselected Softkeys** - Lists softkeys that are associated with a call state. This field lists the unselected, optional softkeys of the call state that displays in the Select a Call State to Configure drop-down list box. The softkeys that are listed in this field get added to the Selected Softkeys field by using the right arrows. You can add the Undefined softkey more than once to the Selected Softkey list. Choosing Undefined results in a blank softkey on the Cisco Unified IP Phone.

• **Selected Softkeys** - Lists softkeys that are associated with the chosen call state. This field lists the chosen softkeys of the call state that displays in the Select a Call State to Configure drop-down list box. The maximum number of softkeys in this field cannot exceed 16. See the figure which follows for a sample softkey layout.

![Figure 47: Sample Softkey Layout](image)

**Softkey template operation**

For applications such as Cisco Unified Communications Manager Assistant to support softkeys, ensure softkeys and softkey sets are configured in the database for each device that uses softkey templates and the application.
You can mix application and call-processing softkeys in any softkey template. A static softkey template associates with a device in the database. When a device registers with Cisco Unified Communications Manager, the static softkey template gets read from the database into call processing and then gets passed to the device to be used throughout the session (until the device is no longer registered or is reset). When a device resets, it may get a different softkey template or softkey layout because of updates that the administrator makes.

Softkeys support a field called application ID. An application, such as Cisco Unified Communications Manager Assistant, activates/deactivates application softkeys by sending a request to the device through the Cisco CTIManager and call processing with a specific application ID.

When a user logs in to the Cisco IP Manager Assistant service and chooses an assistant for the service, the application sends a request to the device, through Cisco CTIManager and call processing, to activate all its softkeys with its application ID.

At any time, several softkey sets may display on a Cisco Unified IP Phone (one set of softkeys for each call). The softkey template that is associated with a device (such as a Cisco Unified IP Phone) in the database designates the one that is used when the device registers with call processing. Perform the association of softkey templates and devices by using Softkey Template configuration in Cisco Unified Communications Manager Administration.

Common phone profiles

Cisco Unified Communications Manager uses common phone profiles to define phone attributes that are associated with Cisco Unified IP Phones. Having these attributes in a profile instead of adding them individually to every phone decreases the amount of time that administrators spend configuring phones and allows the administrator to change the values for a group of phones. Common phone profiles specify the following attributes:

- Profile name
- Profile description
- Local phone unlock password
- DND option
- DND incoming call alert
- Phone personalization
- End user access to phone background image setting

The common phone profile remains a required field when phones are configured; therefore, you must create the common phone profile before you create a phone. Cisco Unified Communications Manager provides a Standard Common Phone Profile that you can copy and modify to create a new common phone profile. You cannot modify nor delete the Standard Common Phone Profile.

Methods for adding phones

You can automatically add phones that support either SCCP or SIP to the Cisco Unified Communications Manager database by using autoregistration, manually by using the phone configuration windows, or in groups with the Bulk Administration Tool (BAT).
By enabling autoregistration before you begin installing phones, you can automatically add a Cisco Unified IP Phone to the Cisco Unified Communications Manager database when you connect the phone to your IP telephony network. During autoregistration, Cisco Unified Communications Manager assigns the next available sequential directory number to the phone. In many cases, you may not want to use autoregistration; for example, if you want to assign a specific directory number to a phone or if you plan to implement authentication or encryption.

Tip
Cisco Unified Communications Manager automatically disables autoregistration if you configure the clusterwide security mode for authentication and encryption through the Cisco CTL client.

If you do not use autoregistration, you must manually add phones to the Cisco Unified Communications Manager database or use the Bulk Administration Tool (BAT). BAT enables system administrators to perform batch add, modify, and delete operations on large numbers of Cisco Unified IP Phones.

Tip
After you install Cisco Unified Communications Manager, if auto-registration is not enabled and the phone has not been added to the Cisco Unified Communications Manager database, the phone does not attempt to register with Cisco Unified Communications Manager. The phone continues to display the Configuring IP message until auto-registration gets enabled or until the phone gets added to the Cisco Unified Communications Manager database. The Real-Time Monitoring Tool and Cisco Unified Reporting can display information on registered and unregistered devices.

User/Phone Add
You can use the End User, Phone, DN, and LA Configuration window to add a new phone at the same time that you add a new end user. You can associate a directory number (DN) and line appearance (LA) for the new end user by using the same window. To access the End User, Phone, DN, and LA Configuration window, choose the User Management > User/Phone Add menu option.

Note
The End User, Phone, DN, and LA Configuration window only allows addition of a new end user and a new phone. The window does not allow entry of existing end users or existing phones.

Phone migration
The Phone Migration window in Cisco Unified Communications Manager Administration allows you to migrate feature, user, and line configuration for a phone to a different phone; that is, you can migrate data to a different phone model or to the same phone model that runs a different protocol. For example, you can migrate data from a Cisco Unified IP Phone 7965 to a Cisco Unified IP Phone 7975; or, you can migrate data from a phone model that runs SCCP, for example, the Cisco Unified IP Phone 7965 (SCCP), and move it to the same phone model that runs SIP, for example, the Cisco Unified IP Phone 7965 (SIP).

Tip
Phone migration allows you to move existing phone configuration to a new phone without the need to add a phone, lines, speed dials, and so on.

Before you can migrate phone configuration to a new phone, consider the following information:
• If the phone models do not support the same functionality, be aware that you may lose functionality on the new phone. Before you save the migration configuration in the Phone Migration window, Cisco Unified Communications Manager Administration displays a warning that you may lose feature functionality.

• Some phone models do not support phone migration; for example, CTI port, H.323 client, Cisco Unified Mobile Communicator, and Cisco IP Softphone.

• Before you can migrate the phone configuration, you must create a phone template for the phone model to which you want to migrate in BAT (Bulk Administration > Phones > Phone Template). For example, if you want to migrate the configuration for a Cisco Unified IP Phone 7965 to a Cisco Unified IP Phone 7975, you create the phone template for the Cisco Unified IP Phone 7975.

• The new phone uses the same existing database record as the original phone, so migrating the phone configuration to the new phone removes the configuration for the original phone from Cisco Unified Communications Manager Administration/the Cisco Unified Communications Manager database; that is, you cannot view or access the configuration for the original phone after the migration.

Migrating to a phone that uses fewer speed dials or lines does not remove the speed dials or lines for the original phone from Cisco Unified Communications Manager Administration/the Cisco Unified Communications Manager database, although some of the speed dials/lines do not display on the new phone. After you migrate the configuration, you can see all speed dials and lines for the original phone in the Phone Configuration window for the new phone.

• Before you migrate the phone configuration to a new phone, ensure that the phones are unplugged from the network. After you perform the migration tasks, you can plug the new phone into the network.

• Before you migrate the phone configuration to a new phone, ensure that you have enough device license units for the new phone.

• If you want to migrate the configuration for multiple phones, use the Bulk Administration Tool.

Phone features

Cisco Unified Communications Manager enables you to configure the following phone features on Cisco Unified IP Phones: barge, privacy release, call back, call park, call pickup, immediate divert, join across lines, malicious call identification, quality report tool, service URL, single button barge/cbarge, and speed dial and abbreviated dial.

Agent Greeting

Agent Greeting enables Cisco Unified Communications Manager to automatically play a pre-recorded announcement following a successful media connection to the agent device. The greeting helps keep agents sounding fresh because they do not have to repeat common phrases on each call. Agent Greeting is audible for the agent and the customer.

If you want to use agent greeting, Built-in Bridge must be On.

Audible Message Waiting Indicator (AMWI)

You can configure Cisco Unified IP Phones, so if voice messages are waiting, the end users will receive a stutter dial tone when the phone goes off hook (on the line on which the voice message has been left) by
setting the Audible Message Waiting Indicator Policy service parameter in Cisco Unified Communications Manager Administration.

---

**Note**

To ensure backward compatibility, the Cisco Unified IP Phones that are running SCCP will not issue the AMWI stutter dial-tone for phones that are using SCCP firmware versions older than 10. This remains true regardless whether the AMWI is configured on the Cisco Unified Communications Manager Administration window.

---

**Barge and Privacy**

The Barge and Privacy features work together. Both features work with phones that run SIP or SCCP by using only shared lines.

Barge adds a user to a call that is in progress. Pressing the Barge or cBarge softkey automatically adds the user (initiator) to the shared-line call (target), and the users currently on the call receive a tone.

Privacy allows a user to allow or disallow other users of shared-line devices to view the device call information or to allow another user to barge in to its active calls.

---

**Calling Party Normalization**

In line with E.164 standards, calling party normalization enhances the dialing capabilities of some phones and improves call back functionality when a call is routed to multiple geographical locations; that is, the feature ensures that the called party can return a call without having to modify the directory number in the call log directories on the phone. Additionally, calling party normalization allows you to globalize and localize phone numbers, so the appropriate calling number presentation displays on the phone.

Configuring calling party normalization alleviates issues with toll bypass where the call is routed to multiple locations over the IP WAN. In addition, it allows Cisco Unified Communications Manager to distinguish the origin of the call to globalize or localize the calling party number for the phone user.

The phone itself can localize the calling party number. For the phone to localize the calling party number, you must configure the Calling Party Transformation CSS or the Use Device Pool Device Calling Party Transformation CSS setting in the Phone Configuration window.

You can configure the international escape character, +, to globalize the calling party number.

**Related Topics**

- Use the international escape character, on page 161

---

**Call Forward**

Call forward allows a user to configure a Cisco Unified IP Phone, so all calls that are destined for it ring another phone. Configure call forward in the Directory Number Configuration window in Cisco Unified Communications Manager Administration.
You can configure each call forward type for internal and external calls and can forward calls to voice-messaging system or a dialed destination number by configuring the calling search space.

The administrator configures call forward information display options to the original dialed number or the redirected dialed number, or both. The administrator enables or disables the calling line ID (CLID) and calling name ID (CNID). The display option gets configured for each line appearance.

---

**Tip**

Call Forward All, including CFA Destination Override, CFA Loop Prevention, and CFA Loop Breakout

Call Forward All (CFA) allows a phone user to forward all calls to a directory number.

The administrator can configure CFA for internal and external calls and can forward calls to a voice-messaging system or a dialed destination number by configuring the calling search space. Cisco Unified Communications Manager includes a secondary Calling Search Space (CSS) configuration field for Call Forward All (CFA). The secondary CSS for CFA combines with the existing CSS for CFA to allow support of the alternate CSS system configuration. When CFA is activated, only the primary and secondary CSS for CFA get used to validate the CFA destination and redirect the call to the CFA destination. If these fields are empty, the null CSS gets used. Only the CSS fields that are configured in the primary CSS for CFA and secondary CSS for CFA fields get used. If CFA is activated from the phone, the CFA destination gets validated by using the CSS for CFA and the secondary CSS for CFA, and the CFA destination gets written to the database. When a CFA is activated, the CFA destination always gets validated against the CSS for CFA and the secondary CSS for CFA.

Cisco Unified Communications Manager provides a service parameter (CFA Destination Override) that allows the administrator to override Call Forward All (CFA) when the target of the CFA calls the initiator of the CFA, so the CFA target can reach the initiator for important calls. In other words, when the user to whom calls are being forwarded (the target) calls the user whose calls are being forwarded (the initiator), the phone of the initiator rings instead of the call being forwarded back to the target. The override works whether the CFA target phone number is internal or external.

When the CFA Destination Override service parameter is set to False (the default value), no override occurs. Ensure the service parameter is set to True for CFA override to work.

---

**Note**

CFA override only takes place if the CFA destination matches the calling party and the CFA Destination Override service parameter is set to True. If the service parameter is set to True and the calling party does not match the CFA destination, CFA override does not take place, and the CFA remains in effect.

---

Cisco Unified Communications Manager prevents Call Forward All activation on the phone when a Call Forward All loop is identified. For example, Cisco Unified Communications Manager identifies a call forward loop when the user presses the CFwdALL softkey on the phone with directory number 1000 and enters 1001 as the CFA destination, and 1001 has forwarded all calls to directory number 1002, which has forwarded all calls to directory number 1003, which has forwarded all calls to 1000. In this case, Cisco Unified Communications Manager identifies that a loop occurs and prevents CFA activation on the phone with directory number 1000.
If Call Forward All activation occurs in Cisco Unified Communications Manager Administration or the Cisco Unified CM User Options windows, Cisco Unified Communications Manager does not prevent the CFA loop.

If the same directory number exists in different partitions, for example, directory number 1000 exists in partitions 1 and 2, Cisco Unified Communications Manager allows the CFA activation on the phone.

The Forward Maximum Hop Count service parameter, which supports the Cisco CallManager service, specifies the maximum number of call hops that can occur for a Call Forward All chain; for example, if the value of this parameter equals 7, and a Call Forward All chain occurs consecutively from directory numbers 1000 to 1007, which equals 7 hops, Cisco Unified Communications Manager prevents a phone user with directory number 2000 from activating CFA to directory number 1000 because no more than 7 forwarding hops are supported for a single call. For more information on this service parameter, including special considerations for calls that use Q.SIG trunks, click the Forward Maximum Hop Count link in the Service Parameter Configuration window in Cisco Unified Communications Manager Administration.

Cisco Unified Communications Manager prevents Call Forward All loops if CFA is activated from the phone, if the number of hops for a Call Forward All call exceeds the value that is specified for the Forward Maximum Hop Count service parameter, and if all phones in the forwarding chain have CFA activated [not Call Forward Busy (CFB), Call Forward No Answer (CFNA), or any other call forwarding options]. For example, if the user with directory number 1000 forwards all calls to directory number 1001, which has CFB and CFNA configured to directory number 1002, which has CFA configured to directory number 1000, Cisco Unified Communications Manager allows the call to occur because directory number 1002 acts as the CFB and CFNA (not CFA) destination for directory number 1001.

Call Forward All loops do not impact call processing because Cisco Unified Communications Manager supports CFA loop breakout, which ensures that if a CFA loop is identified, the call goes through the entire forwarding chain, breaks out of the Call Forward All loop, and completes as expected, even if CFNA, CFB, or other forwarding options are configured along with CFA for one of the directory numbers in the forwarding chain. For example, the user for the phone with directory number 1000 forwards all calls to directory number 1001, which has forwarded all calls to directory number 1002, which has forwarded all calls to directory number 1000, thus creating a CFA loop. In addition, directory number 1002 has configured CFNA to directory number 1004. The user at the phone with directory number 1003 calls directory number 1000, which forwards to 1001, which forwards to 1002. Cisco Unified Communications Manager identifies a CFA loop, and the call, which breaks out of the loop, tries to connect to directory number 1002. If the No Answer Ring Duration timer expires before the user for the phone with directory number 1002 answers the call, Cisco Unified Communications Manager forwards the call to directory number 1004.

For a single call, Cisco Unified Communications Manager may identify multiple Call Forward All loops and attempts to connect the call after each loop is identified.

**Call Forward Busy**

The Call Forward Busy (CFB) feature forwards calls only when the line is in use and the busy trigger setting is reached.

The call forward busy trigger gets configured for each line appearance and cannot exceed the maximum number of calls that are configured for a line appearance. The call forward busy trigger determines how many active calls exist on a line before the call forward busy setting gets activated (for example, 10 calls).
Keep the busy trigger slightly lower than the maximum number of calls, so users can make outgoing calls and perform transfers.

If a call gets forwarded to a directory number that is busy, the call does not complete.

**Call Forward No Answer**

The Call Forward No Answer (CFNA) feature forwards calls when the phone is not answered after the configured no answer ring duration timer is exceeded or if the destination is unregistered.

The call forward no answer ring duration gets configured for each line appearance, and the default specifies 12 seconds. The call forward no answer ring duration determines how long a phone rings before the call forward no answer setting gets activated.

**Call Forward No Coverage**

The Call Forward No Coverage feature forwards calls when ringing either exhausts or times out and the associated hunt-pilot for coverage specifies Use Personal Preferences for its final forwarding.

**Call Waiting**

Call waiting feature lets users receive a second incoming call on the same line without disconnecting the first call. When the second call arrives, the user receives a brief call-waiting indicator tone, which is configured with the Ring Setting (Phone Active) in the Directory Number Configuration window.

Configure call waiting in the Directory Number Configuration window in Cisco Unified Communications Manager Administration by setting the busy trigger (greater than 2) and maximum number of calls.

**Cancel Call Waiting**

The Cancel Call Waiting feature allows the user to cancel the call waiting service when a call is active. This feature enables the user to block the operation of call waiting for one call. To invoke this feature, the user dials the cancel call waiting code, obtains recall dial tone, and places a call normally. During this call, the Call Waiting service is rendered inactive, so that anyone calling the user receives the normal busy treatment, and no call waiting tones interrupt the call.

This feature is available on both IP and analog phones.

The administrator can enable the Cancel Call Waiting feature through a Cancel Call Waiting softkey in Cisco Unified Communications Manager, which adds a new softkey to non-standard softkey templates. The administrator then assigns the template to supported devices.

For more information on softkey templates, see the Softkey templates, on page 514.
Call Diagnostics and Voice-Quality Metrics

You can configure Cisco Unified IP Phones that are running SCCP and SIP to collect call diagnostics and voice-quality metrics by setting the Call Diagnostics Enabled service parameter in Cisco Unified Communications Manager Administration.

SIP fully supports Call Diagnostics and Voice Quality Metrics on Cisco Unified IP Phones. Support includes end-of-call reporting, midcall reporting (for example, call hold, media disconnect), and voice quality metrics. Cisco Unified IP Phones 7940 and 7960 that are running SIP do not report voice quality metrics or midcall reporting. To enable voice quality metrics on Cisco Unified IP Phones for SIP, check the Call Stats check box on the SIP Profile Configuration window.

Call Park

Call park allows a user to place a call on hold, so anyone who is configured to use call park on the Cisco Unified Communications Manager system can retrieve it.

For example, if a user is on an active call at extension 1000, the user can park the call to a call park extension such as 1234, and another user can dial 1234 to retrieve the call.

To use call park, you must add the call park extension (in this case, 1234) in Cisco Unified Communications Manager Administration when you are configuring phone features.

Call Pickup

Cisco Unified Communications Manager provides the following types of call pickup:

- Call pickup-Allows you to answer a ringing phone in your designated call pickup group.
- Group call pickup-Allows you to answer incoming calls in another pickup group.
- Other group pickup-Allows you to answer incoming calls in a pickup group that is associated with your own group.
- Directed call pickup-Allows you to answer incoming calls directly on a specific directory number (DN) that belongs to a pickup group that is associated with your own group.

All types of call pickup can operate automatically or manually. If the service parameter, Auto Call Pickup Enabled, is enabled, Cisco Unified Communications Manager automatically connects you to the incoming call after you press one of the following softkeys on the phone:

- PickUp-For call pickup (calls in your own pickup group)
- GPickUp-For group call pickup (calls in another pickup group) and directed call pickup (calls in a pickup group that is associated with your own pickup group)
- OPickUp-For other group pickup (calls in a pickup group that is associated with your own pickup group)

After the call pickup feature is automated, you need to use only one keystroke for a call connection except for group call pickup and directed call pickup. For group call pickup, you press the GPickUp softkey on the phone and dial the DN of the other pickup group. For directed call pickup, you press the GPickUp softkey on the phone and dial the DN of the ringing phone that you want to pick up.
CTI applications support monitoring of the party whose call is picked up. CTI applications do not support monitoring of the pickup requester or the destination of the call that is picked up. Hence, Cisco Unified Communications Manager Assistant does not support auto call pickup (one-touch call pickup).

**Note**

You configure the call pickup feature when you are configuring phone features in Cisco Unified Communications Manager.

When you are adding a line, you can indicate the call pickup group. The call pickup group indicates a number that can be dialed to answer calls to this directory number (in the specified partition).

### Call Pickup Notification

This feature allows users to receive an audio and/or visual alert when a call rings on a phone in pickup groups in which they are a member. For multiple-line phones, be aware that the alert is available for pickup groups that are associated with the primary line only.

You can configure the following notification parameters in the Call Pickup Group Configuration window:

- Type of notification (audio, visual, both, or neither)
- Content of the visual notification message (called party identification, calling party identification, both, or neither)
- Number of seconds delay between the time the call comes into the original called party and the notification to the rest of the call pickup group members

In the Directory Number Configuration window, you can configure the type of audio notification that is provided when a phone is idle or in use.

### Call Select

The Select softkey allows a user to select a call for feature activation or to lock the call from other devices that share the same line appearance. Pressing the Select softkey on a selected call deselects the call.

When the call gets selected by a device, it gets put in the Remote-In-Use state on all other devices that share the line appearance. No one can select a call that is in the Remote-In-Use state. In other words, selecting a call instance will lock it from other devices that share the same line appearance.

A special display symbol identifies selected calls.

Call Select supports shared lines for phones that run SIP or SCCP. Select on nonshared lines does not get supported for phones that are running SIP.

### Conference Linking

Advanced ad hoc conferencing allows you to link multiple ad hoc conferences together by adding an ad hoc conference to another ad hoc conference as if it were an individual participant. Two types of conference linking exist: linear and nonlinear.
Conference List

The conference list feature provides a list of participant directory numbers that are in an ad hoc conference. The name of the participant displays if it is configured in Cisco Unified Communications Manager Administration.

Any participant can invoke the conference list feature on the phone and can view the participants. The conference controller can invoke the conference list feature and can view and remove any participant in the conference by using the Remove softkey.

Connected Number Display

When a call routes through a translation or route pattern, routes to a Call Forward All or Call Forward Busy destination, or gets redirected through a call transfer or CTI application, the connected number display updates to show the modified number or redirected number.

The Connected Number Display restriction restricts the connected line ID presentation to dialed digits only for the duration of the call.

Device Mobility

Cisco Unified Communications Manager uses IP subnets and device pools that contain location information to determine a device home location. By linking IP subnets to locations, the system can determine whether a device is at its home location or a remote location and register the device accordingly.

To support device mobility, modifications to the device pool structure separate the user information from the location and mobility information. The device pool contains the information that pertains to the device itself and to device mobility. An added common profile allows you to configure all the user-related information. You must associate each device with the common profile for user based information.

Direct Transfer

Using the DirTrfr and Select softkeys, a user can transfer any two established calls to remove the calls from the IP phone. For more information about Direct Transfer, see the Make and receive multiple calls per directory number, on page 199.

Directed Call Park

Directed Call Park allows a user to transfer a parked call to an available user-selected directed call park number. Configure directed call park numbers in the new Cisco Unified Communications Manager Directed Call Park Configuration window. You can configure phones that support the directed call park Busy Lamp Field (BLF) button to monitor the busy/idle status of specific directed call park numbers. Users can also use the BLF button to speed dial a directed call park number.

A user can retrieve a parked call by dialing a configured retrieval prefix followed by the directed call park number where the call is parked.
Cisco recommends that you treat Call Park (a hold function) and Directed Call Park (a transfer function) as mutually exclusive: enable one or the other, but not both. If you do enable both, ensure that the numbers that are assigned to each are exclusive and do not overlap.

Do Not Disturb

The Do Not Disturb (DND) feature provides the following options:

- **Call Reject** - This option specifies that no incoming call information gets presented to the user. Depending on how you configure the DND Incoming Call Alert parameter, the phone may play a beep or display a flash notification of the call.
- **Ringer Off** - This option turns off the ringer, but incoming call information gets presented to the device, so that the user can accept the call.

When DND is enabled, you can also choose to have the Cisco Unified IP Phone beep or flash to indicate an incoming call. Users can configure DND directly from their Cisco Unified IP Phone or from the Cisco Unified CM User Options window.

When DND is enabled, all new incoming calls with normal priority will honor the DND settings for the device. High-priority calls, such as calls from Cisco Emergency Responder (CER) or calls with Multi-Level Precedence and Preemption (MLPP), will ring on the device. Also, when you enable DND, the auto answer feature gets disabled.

The user can enable and disable DND by using any of the following methods:

- **Softkey**
- **Feature Line Key**
- **Cisco Unified CM User Options windows**

You can enable and disable DND on a per-phone basis in Cisco Unified Communications Manager Administration.

EnergyWise

The EnergyWise feature allows certain Cisco Unified IP Phones to participate in an EnergyWise-enabled system. The phone reports its power usage to the EnergyWise domain to allow the tracking and control of power within the customer premise. The phone supports alternate reduced power modes.

The following Cisco Unified IP Phones support EnergyWise in this release:

- Cisco Unified IP Phone 6901
- Cisco Unified IP Phone 6911
- Cisco Unified IP Phone 6921
- Cisco Unified IP Phone 6941
- Cisco Unified IP Phone 6945
- Cisco Unified IP Phone 6961
In the Cisco Unified IP Phones, the EnergyWise feature enables the phone to sleep and wake. A sleeping phone reduces energy consumption, typically into the 0 to 1 watt range.

**Limitations**

You must configure the call manager to power off or power on the Cisco Unified IP Phones at least 12-13 minutes before you configure the Unified CM to power off or power on. This enables the Unified CM, switch, and Cisco Unified IP Phones to synchronize after powering on. Failure prevents the phones from powering off or entering sleep mode at the configured time.

While configuring the Unified CM, keep a minimum of 20 minutes between power off and power on. Failure prevents the phones from powering on.

**EnergyWise in the Cisco Unified IP Phones 7900 series**

Cisco Unified IP Phone 7900 series phones can be configured to automatically sleep and wake at specific times. When these phones are sleeping, users cannot wake them up.

For more information about Energywise, see the appropriate user guide and administration guide:

- Cisco Unified IP Phone 7900 Series User Guide
- Cisco Unified IP Phone 7900 Series Administration Guide

**EnergyWise in the Cisco Unified IP Phones 6900 8900 and 9900 series**

The Cisco Unified IP Phones 6900, 8900, and 9900 Series support EnergyWise by using configured sleep and wake times. In addition, users can wake a sleeping phone using the Select button.

For more information about Energywise, see the appropriate user guide and administration guide:
Hold Reversion

The Hold Reversion feature alerts a phone user when a held call exceeds a configured time limit. When the held call duration exceeds the limit, Cisco Unified Communications Manager generates alerts, such as a ring or beep, at the phone to remind the user to handle the call. The held call becomes a reverted call when the hold duration exceeds the configured time limit. For example, if you configure this feature to notify you when a call remains on hold past 30 seconds, Cisco Unified Communications Manager sends an alert, such as a ring or beep, to the phone after 30 seconds. You can also configure reminder alerts at configured intervals. A user can retrieve a reverted call on hold by going off hook, which deactivates the feature.

You configure hold reversion timers and other feature settings in Cisco Unified Communications Manager Administration for the system or for a line.

- The Hold Reversion Duration timer specifies the wait time before a reverted call alert is issued to the holding party phone.
- The Hold Reversion Notification Interval timer specifies the frequency of the periodic reminder alerts to the holding party phone.
- The Reverted Call Focus priority specifies which call type, incoming calls or reverted calls, receives focus for user actions, such as going off hook.

![Note]

SCCP phones support a minimum Hold Reversion Notification Interval (HRNI) of 5 seconds, whereas SIP phones support a minimum of 10 seconds. SCCP phones set for the minimum HRNI of 5 seconds may experience a Hold Reversion Notification ring delay of 10 seconds when handling calls involving SIP phones.

Immediate Divert

The Immediate Divert feature allows the invoker to immediately divert a call to a voice-messaging system. Managers and assistants, or anyone who shares lines, use this feature. When the call gets diverted, the line becomes available to make or receive new calls.

If the Use Legacy iDivert service parameter is set to False, the invoker can select a party voice mailbox to which to divert an incoming call. The invoker can choose between the original called party voice mailbox or the voice mailbox of the invoker.

To access the Immediate Divert feature, use the iDivert or Divert softkey. Configure the iDivert softkey by using the Softkey Template Configuration window of Cisco Unified Communications Manager Administration (the Divert softkey is not configurable; it displays automatically on the supported phone model such as Cisco...
Unified IP Phone 9971). The softkey template gets assigned to phones that are in the Cisco Unified Communications Manager system.

**Intercom**

Intercom allows a user to place a call to a predefined target. The called destination auto-answers the call in speakerphone mode with mute activated. This sets up a one-way voice path between the initiator and the destination, so the initiator can deliver a short message, regardless whether the called party is busy or idle. To ensure that the voice of the called party is not sent back to the caller when the intercom call is automatically answered, Cisco Unified Communications Manager implements whisper intercom. Whisper intercom means that only one-way audio exists from the caller to the called party. The called party must manually press a key to talk to the caller.

**Internet Protocol Version 6 (IPv6)**

Internet Protocol version 6 (IPv6), which is the latest version of the Internet Protocol (IP) that uses packets to exchange data, voice, and video traffic over digital networks, increases the number of network address bits from 32 bits in IPv4 to 128 bits. IPv6 support in the Cisco Unified Communications Manager network allows the network to behave transparently in a dual-stack environment and provides additional IP address space and autoconfiguration capabilities to devices that are connected to the network.

Cisco Unified IP Phones that run SIP support IPv4 only. Cisco Unified IP Phones that run SCCP can support IPv6 only, IPv4 only, or IPv4 and IPv6 in dual-stack mode.

**Join**

By using the Join softkey, a user can join up to 15 established calls (for a total of 16) to create a conference.

**Join Across Lines**

The Join Across Lines feature allows a user to join calls on multiple phone lines (either on different directory numbers or on the same directory number but on different partitions) to create a conference.

**Log Out of Hunt Groups**

The Log Out of Hunt Groups feature allows phone users to log their phones out from receiving calls that get routed to directory numbers that belong to line groups to which the phone lines are associated. Regardless of the phone status, the phone rings normally for incoming calls that are not calls to the line group(s) that are associated with the phone. The phone provides a visual status of the login state, so the user can determine by looking at the phone whether they are logged in to their line group(s).

The Log Out of Hunt Groups feature also comprises the following components:

- The HLog softkey allows a phone user to log a phone out of all line groups to which the phone directory numbers belong. Configure the HLog softkey in the Softkey Layout Configuration window. When the user presses the HLog softkey, the phone screen displays “Logged out of Hunt Group.” When the user presses the HLog softkey again to log back in and receive hunt group calls, the “Logged out of Hunt Group” notification on the phone screen clears.
To enable this feature, you must configure the Hunt Group Logoff Notification service parameter, which supports the Cisco CallManager service, in the Clusterwide Parameters (Device - Phone) section of the Service Parameters Configuration window.

The Log Out of Hunt Groups feature, which is device-based, operates differently for non-shared lines than for shared lines.

Malicious Call Identification (MCID)

The MCID feature provides a useful method for tracking troublesome or threatening calls. When a user receives this type of call, the Cisco Unified Communications Manager system administrator can assign a new softkey template that adds the Malicious Call softkey to the user phone. For POTS phones that are connected to a SCCP gateway, users can use a hookflash and enter a feature code of *39 to invoke the MCID feature.

Mobile Connect and Mobile Voice Access

The Cisco Unified Mobility Mobile Connect feature enables users to manage business calls by using a single phone number and to pick up in-progress calls on the desktop phone and mobile phone. The Cisco Unified Mobility Mobile Voice Access feature extends mobile connect capabilities by way of an integrated voice response (IVR) system that is used to initiate mobile connect calls and to activate or deactivate mobile connect capabilities.

Monitoring and Recording

Cisco Unified Communications Manager supports silent call monitoring and call recording.

Call centers need to be able to guarantee the quality of customer service that an agent in a call center provides. To protect themselves from legal liability, call centers need to be able to archive agent-customer conversations.

The Silent Call Monitoring feature allows a supervisor to eavesdrop on a conversation between an agent and a customer without allowing the agent to detect the monitoring session.

The Call Recording feature allows system administrators or authorized personnel to archive conversations between the agent and the customer.

Onhook Call Transfer

The Onhook Call Transfer feature supports the onhook (hangup) action as a possible last step to complete a call transfer. You must set the Transfer On-hook Enabled service parameter, which enables onhook call transfer, to True for onhook call transfer to succeed. If the service parameter is set to False, the onhook action ends the secondary call to the third party.

In the existing implementation, if user B has an active call on a particular line (from user A) and user B has not reached the maximum number of calls on this line, the Cisco Unified IP Phone provides a Transfer softkey to user B. If user B presses the Transfer softkey (or Transfer button, if available) once, user B receives dial tone and can make a secondary call: user B dials the number of a third-party (user C). Cisco Unified Communications Manager provides a Transfer softkey to user B again. If user B presses the Transfer softkey again (or Transfer button, if available), the transfer operation completes.

With the onhook call transfer implementation, user B can hang up after dialing the number of user C, and the transfer completes. Both the existing and new implementations work in the case of a blind transfer (user B
disconnects before user C answers) and also in the case of a consult transfer (user B waits for user C to answer and announces the call from user A).

The previous implementation remains unchanged: user B can press the Transfer softkey twice to complete the transfer.

**Prime Line Support for Answering Calls**

With prime line support for answering calls, when the phone is idle (off hook) and receives a call on any line, the primary line always gets chosen for the call. When you configure this support, going off hook makes only the first line active, even when a call rings on another line on the phone; that is, the call does not get answered on that line. In this case, the phone user must choose the other line to answer the call.

You can configure the Always Use Prime Line service parameter for the Cisco CallManager service or you can configure the Always Use Prime Line setting for devices and device profiles. The Always Use Prime Line setting displays in the following windows in Cisco Unified Communications Manager Administration.

- System > Service Parameters (for Cisco CallManager service)
- Device > Phone
- Device > Common Phone Profile
- Device > Device Settings > Default Device Profile
- Device > Device Settings > Device Profile

For information on how the Always Use Prime Line setting works when a phone is idle or busy, see the following table.

### Tip
If you configure the Always Use Prime Line setting in the Service Parameter, Common Phone Profile, and in the Phone Configuration window, Cisco Unified Communications Manager uses the configuration from the Phone Configuration window.

<table>
<thead>
<tr>
<th>State of Phone</th>
<th>Configuration for Always Use Prime Line</th>
<th>How Feature Works</th>
</tr>
</thead>
<tbody>
<tr>
<td>Idle</td>
<td>On</td>
<td>When the phone is idle (off hook) and receives a call on any line, the primary line gets chosen for the call. Calls on other lines continue to ring, and the phone user must select those other lines to answer these calls. If you choose On for the Always Use Prime Line setting in the Device Profile or Default Device Profile Configuration window, a Cisco Extension Mobility user can use this feature after logging in to the device that supports Cisco Extension Mobility; that is, if you configure Cisco Extension Mobility correctly.</td>
</tr>
</tbody>
</table>
How Feature Works

<table>
<thead>
<tr>
<th>State of Phone</th>
<th>Configuration for Always Use Prime Line</th>
<th>How Feature Works</th>
</tr>
</thead>
<tbody>
<tr>
<td>Idle</td>
<td>Off</td>
<td>When the phone is idle and receives a call on any line, the phone user answers the call from the line on which the call is received; that is, when the phone is off hook.</td>
</tr>
<tr>
<td>Idle</td>
<td>Default</td>
<td>If you choose Default for the Always Use Prime Line setting in the Common Phone Profile, the Device Profile, or the Default Device Profile Configuration windows, Cisco Unified Communications Manager uses the configuration from the Always Use Prime Line service parameter when determining whether a user, including a Cisco Extension Mobility user, can use this feature. If you choose Default for the for the Always Use Prime Line setting in the Phone Configuration window, Cisco Unified Communications Manager uses the configuration from the common phone profile.</td>
</tr>
<tr>
<td>Busy</td>
<td>On</td>
<td>When the phone already has a call on a line, Cisco Unified Communications Manager uses the configuration for the Maximum Number of Calls and Busy Trigger settings to determine how to route the call.</td>
</tr>
<tr>
<td>Idle</td>
<td>On, but you also configured Auto Answer With Headset or Auto Answer with Speakerphone</td>
<td>If you choose the Auto Answer with Headset option or Auto Answer with Speakerphone option from the Auto Answer drop-down list box in Cisco Unified Communications Manager Administration, the Auto Answer configuration overrides the configuration for the Always Use Prime Line setting.</td>
</tr>
</tbody>
</table>

Tip
This feature relies on the Cisco CallManager service, so activate the service by choosing Tools > Service Activation in Cisco Unified Serviceability. In addition, you can run SDI trace for the Cisco CallManager service. When you view the log in RTMT, you can see the configured value that is used by the device; for example, alwaysPrimeLine=1, which indicates that the device uses On for the configuration.

Note
If you want to do so, you can configure prime line support for answering calls in the Bulk Administration Tool.

Peerto-Peer Image Distribution (PPID)

The Peer Firmware Sharing feature provides these advantages in high-speed campus LAN settings:

- Limits congestion on TFTP transfers to centralized TFTP servers.
• Eliminates the need to manually control firmware upgrades.
• Reduces phone downtime during upgrades when large numbers of devices are reset simultaneously.

In most conditions, the Peer Firmware Sharing feature optimizes firmware upgrades in branch deployment scenarios over bandwidth-limited WAN links.

When the feature is enabled, it allows the phone to discover like phones on the subnet that are requesting the files that make up the firmware image and to automatically assemble transfer hierarchies on a per-file basis. The individual files that make up the firmware image get retrieved from the TFTP server by only the root phone in the hierarchy and are then rapidly transferred down the transfer hierarchy to the other phones on the subnet using TCP connections.

Configure PPID from the Phone Configuration window by using the Peer Firmware Sharing settings in the Product-Specific Configuration Layout. This menu option indicates whether the phone supports PPID. Settings include enabled or disabled (the default).

To configure the PPID feature for many phones, use the Peer Firmware Settings field in the Phone Template window of the Bulk Administration Tool.

For more information, see the applicable Cisco Unified IP Phone administration guide.

Quality Report Tool

The Quality Report Tool (QRT), a voice-quality and general problem-reporting tool for Cisco Unified IP Phones, allows users to easily and accurately report audio and other general problems with their IP phone. QRT gets loaded as part of the Cisco Unified Communications Manager installation, and the Cisco Extended Functions (CEF) service supports it.

As system administrator, you enable QRT functionality by creating, configuring, and assigning a softkey template to associate the QRT softkey on a user IP phone. You can choose from two different user modes, depending upon the level of user interaction that you want with QRT. You then define how the feature will work in your system by configuring system parameters and setting up Cisco Unified Serviceability tools. You can create, customize, and view phone problem reports by using the QRT Viewer application.

Support for the QRT feature extends to any IP phone that includes the following capabilities:

• Support for softkey templates
• Support for IP phone services
• Controllable by CTI
• Contains an internal HTTP server

When users experience problems with their IP phones, they can report the type of problem and other relevant statistics by pressing the QRT softkey on the Cisco Unified IP Phone during one of the following call states:

• Connected
• Connected Conference
• Connected Transfer
• On Hook
From a supported call state, and using the appropriate problem classification category, a user can then choose the reason code that best describes the problem that is being reported for the IP phone. A customized phone problem report provides you with the specific information.

**Secure Tone**

You can configure a phone to play a 2-second tone that notifies the user that a call is encrypted and that both phones on the call are configured as “protected” devices. The tone plays for both parties when the call is answered. The tone does not play unless both phones are “protected” and the call occurs over encrypted media. Several configuration requirements exist for the secure tone to play.

**Service URL**

You can configure a Cisco Unified IP Phone Service URL, such as the extension mobility service, to a phone button. When the button gets pressed, the service gets invoked.

To configure a service URL on a phone button for the user, the administrator performs the following steps:

1. Using IP Phone Services Configuration, create a service.
2. Using Phone Button Configuration, create a custom phone button template to include the service URL feature.
3. Using Phone Configuration, add the custom phone button template to each phone that requires the service URL button.
4. Using Phone Configuration, subscribe to each appropriate service.
5. Using Phone Configuration, add the service URL button.
6. Notify the users to configure services for their phone by using the Add/Update your Service URL Buttons link on the User Options Menu.

**Single Button Barge/cBarge**

The Single Button Barge/cBarge and Privacy features work together. These features work by using only shared lines.

The Barge and cBarge features add a user to a call that is in progress. The Single Button Barge/cBarge feature allows a user to simply press the shared-line button of a call to automatically add that user to the call. The users that are currently on the call receive a tone.

Privacy allows a user to allow or disallow other users of shared-line devices to view the device call information or to allow another user to barge in to its active calls.

**Speed Dial and Abbreviated Dial**

Cisco Unified Communications Manager supports the configuration of up to 199 speed-dial entries, which are accessed through phone buttons and abbreviated dialing.

The administrator configures speed-dial entries and abbreviated dial indexes in the same window. From the Phone Configuration window, choose Add/Update Speed Dials from the Related Links drop-down list box.
at the top of the window and click Go. The Speed Dial and Abbreviated Dial Configuration window displays for this phone.

When the user configures speed-dial entries, part of the speed-dial entries can get assigned to the speed-dial buttons on the IP phone; the remaining speed-dial entries get used for abbreviated dialing. When a user starts dialing digits, the AbbrDial softkey displays, and the user can access any speed-dial entry by entering the appropriate index (code) for abbreviated dialing.

When users configure speed-dial in Cisco Unified CM User Options, 199 entries display. Depending on the phone type, up to a maximum of 107 speed-dials can be used. Speed dials for which there is no corresponding button on the phone can only be accessed by using the Abbreviated Dial feature, if available.

Table 50: Maximum Speed Dials per Phone Model

<table>
<thead>
<tr>
<th>Phone Model</th>
<th>Maximum Number of Speed-Dial Entries Available on the Phone</th>
<th>Maximum Number of Speed-Dial Entries Available with Expansion Modules</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Unified IP Phone 9971</td>
<td>4</td>
<td>107</td>
</tr>
<tr>
<td>Cisco Unified IP Phone 9951</td>
<td>3</td>
<td>71</td>
</tr>
<tr>
<td>Cisco Unified IP Phone 8961</td>
<td>3</td>
<td>35</td>
</tr>
<tr>
<td>Cisco Unified IP Phone 7975</td>
<td>6</td>
<td>55</td>
</tr>
<tr>
<td>Cisco Unified IP Phone 7965, 7962</td>
<td>4</td>
<td>53</td>
</tr>
<tr>
<td>Cisco Unified IP Phone 7960</td>
<td>4</td>
<td>35</td>
</tr>
</tbody>
</table>

Note: Maximum number of speed-dial entries available on the phone is equal to maximum number of buttons available on the phone minus one button for Line 1.

VPN Client

The VPN Client feature establishes a virtual private network (VPN) connection on your phone using the Secure Sockets Layer (SSL). The VPN connection is used for situations in which a phone is located outside a trusted network or when network traffic between the phone and Cisco Unified Communications Manager must cross untrusted networks.

After the phone gets configured with VPN functionality and the VPN feature gets enabled, the user enters credentials as follows:

- If the phone is located outside the corporate network—The user is prompted at login to enter the credentials based on the authentication method that the system administrator configured on the phone.
- If the phone is located inside the corporate network:
  - If Auto Network Detection is disabled, the user is prompted for credentials, and a VPN connection is possible.
If Auto Network Detection is enabled, the user cannot connect through VPN so there is no prompt.

The user can enable or disable the VPN Client mode on the phone.

You can use Cisco Unified Reporting to determine which Cisco Unified IP Phones support the VPN client. From Cisco Unified Reporting, click Unified CM Phone Feature List. For the Feature, choose Virtual Private Network Client from the pull-down menu. The system displays a list of products that support the feature.

**Whisper Coaching**

Silent call monitoring is a feature that allows a supervisor to discreetly listen to a conversation between an agent and a customer without allowing the agent to detect the monitoring session. Whisper coaching is an enhancement to silent call monitoring feature that allows supervisors to talk to agents during a monitoring session. This feature provides applications the ability to change the current monitoring mode of a monitoring call from Silent Monitoring to Whisper Coaching and vice versa.

To invoke whisper coaching, choose On from the built-in bridge drop-down list (Device > Phone).

**Phone association**

Users can control some devices, such as phones. Applications that are identified as users control other devices, such as CTI ports. When users have control of a phone, they can control certain settings for that phone, such as speed dial and call forwarding.

**Phone administration tips**

The following sections contain information that may help you configure phones in Cisco Unified Communications Manager Administration.

**Phone search**

The following sections describe how to modify your search to locate a phone. If you have thousands of Cisco Unified IP Phones in your network, you may need to limit your search to find the phone that you want. If you are unable to locate a phone, you may need to expand your search to include more phones.

---

**Note**

Be aware that the phone search is not case sensitive.

---

**Searching by Device Name**

When you enter the MAC address of the device in the MAC Address field when you are adding the phone, you can search by using that value as the Device Name in the Find and List Phones window.

**Searching by Description**

If you enter a user name and/or extension in the Description field when you are adding the phone, you can search by using that value in the Find and List Phones window.
Searching by Directory Number

To search for a phone by its directory number (DN), choose Directory Number. Choose a search criterion (such as begins with or ends with) and either choose a directory number from the drop-down list box below the **Find** button or enter a search string. Click the **Find** button to perform the search.

**Note**

Some directory numbers do not associate with phones. To search for those directory numbers, which are called unassigned DN, use the Route Plan Report window or use the Directory Number Configuration Find/List window.

Searching by Calling Search Space

If you choose calling search space, the options that are available in the database display; you can choose one of these options from the drop-down list box below the **Find** button.

Searching by Device Pool

If you choose device pool, the options that are available in the database display (for example, Default); you can choose one of these options from the drop-down list box below the **Find** button.

Searching by Device Type

To search for a phone by its device type, choose Device Type and either enter a device type or choose a device type from the drop-down list box below the **Find** button.

Searching by Call Pickup Group

To search for a phone by its call pickup group, choose Call Pickup Group. If you choose Call Pickup Group, the options that are available in the database display; you can choose one of these options from the drop-down list box below the **Find** button. Alternatively, click the **Find** button only.

Searching by LSC Status

If you choose LSC status, the options that are available in the database display (for example, Operation Pending); you can choose one of these options from the drop-down list box below the **Find** button.

Searching by Authentication String

To search for a phone by an authentication string, choose Authentication String and enter an authentication string.

Searching by Device Protocol

To search for a phone by the protocol, choose Device Protocol and either enter a protocol, such as SIP, or choose a protocol from the drop-down list box below the **Find** button.

Searching by Security Profile

To search for a phone by its security profile, choose Security Profile and either enter a security profile name or choose a security profile from the drop-down list box below the **Find** button.
Searching by Common Device Configuration

To search for a phone by its common device configuration, choose Common Device Configuration and either enter a common device configuration name or choose a common device configuration from the drop-down list box below the Find button.

Refining Search Criteria

To add additional search criteria, click the + button. When you add criteria, the system searches for a record that matches all criteria that you specify. To remove criteria, click the - button to remove the last added criterion or click the Clear Filter button to remove all added search criteria.

Finding All Phones in the Database

To find all phones that are registered in the database, choose Device Name from the list of fields; choose “is not empty” from the list of patterns; then, click the Find button.

Note

The list in the Find and List Phones window does not include analog phones and fax machines that are connected to gateways (such as a Cisco VG200). This list shows only phones that are configured in Cisco Unified Communications Manager Administration.

Messages button

By performing the following actions, you can configure a voice-messaging access number for the messages button on Cisco Unified IP Phone, so users can access the voice-messaging system by simply pressing the messages button:

1 Configure the voice-mail pilot number by choosing Advanced Features > Voice Mail > Voice Mail Pilot.
2 Configure the voice-mail profile by choosing Advanced Features > Voice Mail > Voice Mail Profile.
3 Choose the appropriate profile from the Voice Mail Profile field on the Directory Number Configuration window. By default, this field uses the default voice-mail profile that uses the default voice-mail pilot number configuration.

Note

Typically, you can edit the default voice-mail pilot and default voice-mail profiles to configure voice-messaging service for your site.

Directories button

The Cisco Unified IP Phone can display directories of names and phone numbers. You access this directory from the directories button on the IP phone. For end users to retrieve contacts from the corporate directory, the administrator must enter users into the directory. Enter the contacts one at a time by using Cisco Unified Communications Manager Administration User Management (User Management > End User). The administrator can also add multiple users in bulk by using the Bulk Administration Tool (Bulk Administration > End User).
Other types of directories exist that can display on the IP phone: personal directory and phone directory (such as missed calls). To find out about these directories, see the user guide for the specific Cisco Unified IP Phone.

The URL Directories enterprise parameter defines the URL that points to the global directory for display on the Cisco Unified IP Phone. The XML device configuration file for the phone stores this URL.

**Tip**
If you are using IP addresses rather than DNS for name resolution, make sure that the URL Directories enterprise parameter value uses the IP address of the server for the hostname.

**Tip**
If the phone URL was not updated correctly after the URL Directories enterprise parameter was changed, try stopping and restarting the Cisco TFTP service; then, reset the phone.

---

### Cisco Unified CM user options

Cisco Unified IP Phone users access Cisco Unified CM User Options through their web browser, so they can configure a variety of features on their phone. Some of the configurable features include user locale, user password, call forward, speed dial, and remote destinations. By setting enterprise parameters as either True or False, you can configure which features are made available to users; for example, you can set the Show Speed Dial Settings enterprise parameter to False, and users cannot configure speed dials on their phones.

---

### Maximum Phone Fallback Queue Depth service parameter

Cisco does not support failover and fallback for Cisco Unified Communications Manager Business Edition 5000 systems. The Cisco CallManager service uses the Maximum Phone Fallback Queue Depth service parameter to control the number of phones to queue on the higher priority Cisco Unified Communications Manager when that Cisco Unified Communications Manager is available for registration. The default specifies 10 phones per second. If a primary Cisco Unified Communications Manager fails, the phones fail over to the secondary Cisco Unified Communications Manager. The failover process happens as fast as possible by using the priority queues to regulate the number of devices that are currently registering.

When the primary Cisco Unified Communications Manager recovers, the phones get returned to that Cisco Unified Communications Manager; however, you do not need to remove a phone from a working Cisco Unified Communications Manager, in this case the secondary system, as fast as possible because the phone remains on a working system. The queue depth gets monitored (using the Maximum Phone Fallback Queue Depth service parameter setting) to determine whether the phone that is requesting registration gets registered now or later. If the queue depth is greater than 10 (default), the phone stays where it is and tries later to register to the primary Cisco Unified Communications Manager.

In the Service Parameters Configuration window, you can modify the Maximum Phone Fallback Queue Depth service parameter. If the performance value is set too high (the maximum setting specifies 500), phone registrations could slow the Cisco Unified Communications Manager real-time response. If the value is set too low (the minimum setting specifies 1), the total time for a large group of phones to return to the primary Cisco Unified Communications Manager will be long.

---

### Dependency records

If you need to find what directory numbers a specific phone is using or to what phones a directory number is assigned, choose Dependency Records from the Related Links drop-down list box on the Cisco Unified
Communications Manager Administration Phone Configuration or Directory Number Configuration window. The Dependency Records Summary window displays information about directory numbers that are using the phone. To find more information about the directory number, click the directory number, and the Dependency Records Details window displays. If the dependency records are not enabled for the system, the dependency records summary window displays a message.

Phone failover and fallback

This section describes how phones fail over and fall back if the Cisco Unified Communications Manager to which they are registered becomes unreachable. This section also covers conditions that can affect calls that are associated with a phone, such as reset or restart.

Cisco does not support failover and fallback for Cisco Unified Communications Manager Business Edition 5000.

Cisco Unified Communications Manager Fails or Becomes Unreachable

The active Cisco Unified Communications Manager designation applies to the Cisco Unified Communications Manager from which the phone receives call-processing services. The active Cisco Unified Communications Manager usually serves as the primary Cisco Unified Communications Manager for that phone (unless the primary machine is not available).

If the active Cisco Unified Communications Manager fails or becomes unreachable, the phone attempts to register with the next available Cisco Unified Communications Manager in the Cisco Unified Communications Manager Group that is specified for the device pool to which the phone belongs.

The phone device reregisters with the primary Cisco Unified Communications Manager as soon as it becomes available after a failure. See the Maximum Phone Fallback Queue Depth service parameter, on page 541 for information about phone registration during failover.

Note

Phones do not fail over or fall back while a call is in progress.

Phone is Reset

If a call is in progress, the phone does not reset until the call finishes.
Chapter 44

Video telephony

This chapter provides information about video telephony. Cisco Unified Communications Manager supports video telephony and thus unifies the world of voice and video calls. Video endpoints use Cisco Unified Communications Manager call-handling features and access a unified voice and video solution for dialing and connecting video calls.

The Cisco Unified Communications Manager video telephony solution offers these features:

• Supports video and video-related features, such as far-end camera control (FECC)
• Supports multiple logical channels that are needed to allow the transmission of video streams
• Transmits midcall, media-related messages that are needed for video (that is, transmits commands or indications that are needed for video calls)
• Supports H.323, Skinny Client Control Protocol (SCCP), and Session Initiation Protocol (SIP)
• Enhances locations and regions to provide bandwidth management
• Provides serviceability information, such as Call Detail Records (CDRs), about video calls

Configure video telephony

Cisco Unified Communications Manager supports video telephony and thus unifies the world of voice and video calls. Video endpoints use Cisco Unified Communications Manager call-handling features and access a unified voice and video solution for dialing and connecting video calls.

The Cisco Unified Communications Manager video telephony solution offers these features:

• Supports video and video-related features, such as far-end camera control (FECC)
• Supports multiple logical channels that are needed to allow the transmission of video streams
• Transmits midcall, media-related messages that are needed for video (that is, transmits commands or indications that are needed for video calls)
• Supports H.323, Skinny Client Control Protocol (SCCP), and Session Initiation Protocol (SIP)
• Enhances locations and regions to provide bandwidth management
• Provides serviceability information, such as Call Detail Records (CDRs), about video calls

To configure video telephony in Cisco Unified Communications Manager Administration follow these steps.

**Procedure**

**Step 1** If you use regions for call admission control, configure regions for video call bandwidth.

**Note** All devices include a default region, which defaults to 384 kb/s for video.

**Tip** Set the bandwidth setting in Region configuration high enough for the desired resolution (for example, increase to 2Mb/s for high-definition video call).

**Step 2** If you use locations for call admission control, configure locations for video call bandwidth.

**Step 3** If using RSVP for bandwidth management of SIP video calls, configure the RSVP service parameters, or set the RSVP policy in the Location Configuration window.

**Step 4** To use a Cisco video conference bridge, configure the appropriate conference bridge for your network.

**Step 5** To configure a user to use the video conference bridge instead of using other conference bridges, configure the media resource groups and media resource group lists for the user accordingly.

**Step 6** Configure the H.323 gateways in your system to retry video calls as audio calls (default behavior) or configure AAR groups and route/hunt lists to use alternate routing for video calls that do not connect.

**Step 7** Configure the H.323 phones in your system to retry video calls as audio calls (default behavior) or configure AAR groups and route/hunt lists to use alternate routing for video calls that do not connect. Choose Enabled for Video Capabilities.

**Step 8** Configure the H.323 trunks in your system to retry video calls as audio calls (default behavior) or configure AAR groups and route/hunt lists to use alternate routing for video calls that do not connect.

**Step 9** Configure the Cisco Unified IP Phones that will support video.

**Step 10** Configure the third-party SIP endpoints that will support video.

**Step 11** Configure the SIP trunks in your system to retry video calls as audio calls (default behavior).

**Related Topics**

- Call admission control, on page 65
- Configuring SIP devices for video calls, on page 556
- Phone configuration for video calls, on page 570

**Introducing video telephony**

The topics in the following section discuss the details of video telephony in the Cisco Unified Communications Manager environment.
Video calls

The typical video call includes two or three Real-Time Protocol (RTP) streams in each direction (that is, four or six streams). The call can include the following stream types:

- Video (H.261, H.263, H.263+, H.264, and Cisco VT Camera wideband video codecs) at a different port
- Far-end camera control (FECC) (optional)

Call control for video calls operates the same way as the call control that governs all other calls. See the Media resources overview, on page 246.

Note

See Intelligent bridge selection, on page 281 for details on how Cisco Unified Communications Manager can allocate a video conference bridge automatically.

Real-Time Transport Control Protocol pass-through

Real-Time Transport Control Protocol pass-through in MTP topologies

An IOS Media Terminating Point (MTP) prior to 15.2(2)T, cannot pass-through Real-Time Transport Control Protocol (RTCP) packets and therefore cannot exchange Real-Time Protocol (RTP) feedback data to enhance the RTP transmission. The primary function of RTCP is to provide feedback of media distribution by periodically sending statistics to participants in a streaming multimedia session. RTCP gathers statistics for a media connection and information such as transmitted octet and packet counts, lost packet counts, jitter, and round-trip delay time. An application may use this information to control quality of service parameters, perhaps by limiting flow, or using a different codec.

IOS MTP Version 15.2(2)T and later supports RTCP pass-through capability so that the endpoint in a call with an MTP present can still provide feedback and status on an RTP transmission. RTCP pass-through capability applies on media channels.

The RTCP pass-through feature is not limited to a specific call signaling protocol. For example it can be SIP-SIP, SIP-nonSIP, or nonSIP-nonSIP.

In order for Cisco Unified CM to allocate an RTCP pass-through capable MTP specifically, the call needs to fulfill the following conditions:

- An MTP is requested for a feature that requires the MTP to be in media pass-through mode. For example, TRP, DTMF translation, IP address V4/V6 translation, etc. RTCP pass-through is only applicable when media is in pass-through mode
- The RTCP pass-through MTP needs to be included in the Media Resource Group Lists (MRGL) of the endpoint that sponsors the MTP. MTP can be inserted by RSVP, E2ERSVP, TRP, DTMF mismatch reasons.
- When the call is capable of establishing video channels, Cisco Unified CM attempts to search for an RTCP pass-through capable MTP. For example, Cisco Unified CM picks an RTCP pass through capable MTP from other non-capable ones in the MRGL. If an RTCP pass-through capable MTP is not available, then Cisco Unified CM still allocates an MTP for the call.
- When the call is capable of establishing an audio channel only, Cisco Unified CM does not intentionally requests an RTCP-pass-through capable MTP for the non-video call. However, if the MRGL only
contains RTCP-pass-through capable MTP(s), then Cisco Unified CM inserts one of those to the audio call.

• In order to have an RTCP pass-through capable MTP, the call also needs to fulfill the current CAC bandwidth for video call.

Note

If a call initially establishes with a non-RTCP pass-through capable MTP (prior to version 15.2(2)T) present in the call, and the call escalates into a video capable call, Cisco Unified CM does not reallocate to an RTCP-pass-through capable MTP. In that case, even though the call has been escalated to a video call, the existing MTP does not allow RTCP packets to be passed through.

Video codecs

Common video codecs include H.261, an older video codec, H.263, a newer codec that gets used to provide internet protocol (IP) video, and H.264, a high-quality codec. The system supports H.264 for calls that use the Skinny Client Control Protocol (SCCP), H.323, and SIP on originating and terminating endpoints only. The system also supports regions and locations.

H.261 and H.263 codecs exhibit the following parameters and typical values:

• Bitrates range from 64 kb/s to a few mb/s. These bitrates can exist in any multiple of 100 b/s. H.261 and H.263 can function with bit rates lower than 64 kb/s, but video quality suffers in such cases.

• Resolution:
  ◦ One-quarter Common Interchange Format (QCIF) (Resolution equals 176x144.)
  ◦ Common Interchange Format (CIF) (Resolution equals 352x288.)
  ◦ 4CIF (Resolution equals 704x576.)
  ◦ Sub QCIF (SQ CIF) (Resolution equals 128x96.)
  ◦ 16CIF (Resolution equals 1408x1152.)
  ◦ Custom Picture Format

• Frame Rate: 15 frames per second (fps), 30 fps

• Annexes: F, D, I, J,K, L, P, T, N

Cisco Unified Video Advantage (CUVA) supports the H.263 and H.264 codecs that can be used for intracluster and intercluster calls, respectively. Correct configuration with related capabilities and regions provides basis for support. This support also applies to mid-call.

The bandwidth of video calls equals the sum of the audio bandwidth and the video bandwidth. The total bandwidth does not include overhead.

Example

A 384-kb/s video call may comprise G.711 at 64 kb/s (for audio) plus 320 kb/s (for video). This sum does not include overhead. If the audio codec for a video call is G.729 (at 24 kb/s), the video rate increases to maintain a total bandwidth of 384 kb/s. If the call involves an H.323 endpoint, the H.323 endpoint may use
less than the total video bandwidth that is available. Regardless of protocol, the endpoint may always choose to send at less than the max bit rate for the call.

**Video network**

The figure which follows provides an example of a video network that uses a single Cisco Unified Communications Manager cluster. In a successful video network, any endpoint can call any other endpoint. Video availability only exists if both endpoints are video enabled. Video capabilities extend across trunks.

*Figure 48: Video Network Example*

The Cisco video conference portfolio comprises the following video bridges:

- Cisco TelePresence MCU series
- ISRG2 ad hoc video conference service
- MeetingPlace

The Cisco UC Endpoints portfolio comprises the following endpoints that support video:

- Cisco Unified IP Phone 9971
- Cisco Unified IP Phone 9951
- Cisco Unified IP Phone 8941
- Cisco Unified IP Phone 8945
- Cisco Unified IP Phone 7985
- Cisco IP Video Phone E20
• Cisco TelePresence EX60
• Cisco TelePresence EX90
• Cisco TelePresence Quick Set C20
• Cisco TelePresence Codec C40
• Cisco TelePresence Codec C60
• Cisco TelePresence Codec C90
• Cisco TelePresence 1000
• Cisco TelePresence 1100
• Cisco TelePresence 1300-47
• Cisco TelePresence 1300-65
• Cisco TelePresence 1310-65
• Cisco TelePresence 3000
• Cisco TelePresence 3200
• Cisco TelePresence 500-32
• Cisco TelePresence 500-37
• Cisco TelePresence MX200
• Cisco TelePresence MX300
• Cisco TelePresence TX9000
• Cisco TelePresence TX9200

For more information, refer to the applicable IP phone user and administration guide.

---

**Note**

Third-party SIP video endpoints are capable of connecting to Cisco Unified Communications Manager as a line-side device or as a trunk-side device. For more information, see [Third-party SIP endpoints](#), on page 479.

---

**Enabling an audio-only device with video**

You can enable an IPv4-only audio-only device with video by using a Cisco application, Cisco Unified Video Advantage. You can associate the application with a Cisco Unified IP Phone in order to display the video component on your PC or laptop. This association can occur before a call is made or during a call (mid-call). Cisco Unified IP Phones, such as 7975, 7940, 7960, 7975, 6961, 6941, and 6921 support Cisco Unified Video Advantage.

For example, a call occurs from a Cisco Unified IP Phone 7975 to a video phone. The call gets established as audio only. After Cisco Unified Video Advantage is associated with the Cisco Unified IP Phone 7975, the call gets reestablished as a video call.
During the association, Cisco Unified Communications Manager receives updated capabilities for the phone via existing SCCP messages. After the updated capabilities are received, Cisco Unified Communications Manager negotiates for video.

If the initial call involves an IP phone without a video, only audio location bandwidth gets reserved, and the media layer establishes an audio-only call.

In addition to audio phones, Cisco video phones, such as 9971 and 9951 also support Cisco Unified Video Advantage.

**H.323 video**

H.323 video exhibits the following characteristics:

- H.323 endpoints can be configured as H.323 phones, H.323 gateways, or H.323 trunks.
- Call forwarding, dial plan, and other call-routing-related features work with H.323 endpoints.
- H.323 video endpoints cannot initiate hold, resume, transfer, park, and other similar features.
- If an H.323 endpoint supports the empty capability set (ECS), the endpoint can be held, parked, and so forth.
- Some vendors implement call setup in such a way that they cannot increase the bandwidth of a call when the call gets transferred or redirected. In such cases, if the initial call is audio, users may not receive video when they are transferred to a video endpoint.
- No video media termination point (MTP) nor video transcoder currently exists. If an audio transcoder or MTP is inserted into a call, that call will be audio only. This is true when the IPVC audio transcoding capabilities is not being used. When the IPVC transcoders are used, you can transcode the audio and send/receive video.
- For H.323 video calls, users must specify video call bandwidth.

**Dynamic H.323 addressing**

You can configure a H.323 client with the E.164 address that is registered with the gatekeeper. E.164 addressing facilitates H.323 configuration and call routing by allowing the Cisco Unified Communications Manager to route all calls in place of the gatekeeper. The gatekeeper that is to be configured requires the following characteristics:

- Forward all calls to the Cisco Unified Communications Manager for routing.
- Calls that are routed from the Cisco Unified Communications Manager must not be routed back to the Cisco Unified Communications Manager.

**Registering with the gatekeeper**

At boot time, Cisco Unified Communications Manager loads static configuration information such as the E.164 address and the configured gatekeeper for each H.323 client. The H.323 clients in the same gatekeeper zone stay in one group. A registration with the gatekeeper gets initiated for the group. The process does not require individual registration for each member of the group.

H.323 clients that belong to the same gatekeeper and zone belong to the same group, and only one registration is initiated for this group. H.323 devices that belong to the same gatekeeper as the first group but to a different
gatekeeper zone are part of another group, and only one registration is initiated for this group. All members of the same group use the same technology prefix.

Call processing

During an outbound call where the H.323 client is the called party, Cisco Unified Communications Manager routes the call on the basis of DN to the H.323 device. Cisco Unified Communications Manager uses the H.323 device configuration to determine whether the gatekeeper is configured and sends an Admission Request Message (ARQ) with the configured E.164 address. If the device is registered with the gatekeeper, the gatekeeper sends an Admission Confirm Message (ACF) with the device's current IP address. Cisco Unified Communications Manager routes the call directly to this address.

During an inbound call where the H.323 device is the calling party, the gatekeeper routes the call to Cisco Unified Communications Manager. Cisco Unified Communications Manager uses the source E.164 address to determine whether the calling device is configured. Cisco Unified Communications Manager uses the configuration to determine the configuration for that phone. The phone configuration includes regions, locations, MRGL, and so on.

Be aware of the following items:

- The system does not support E.164 addressing on H.323 trunks, intercluster trunks, and H.323 gateways.
- Cisco Unified Communications Manager does not resolve the device name when a gatekeeper-controlled H.323 client is configured. Cisco Unified Communications Manager can access the gatekeeper field for the H.323 client to discover the device. This enables Cisco Unified Communications Manager to bypass name resolution for the device name.
- Cisco Unified Communications Manager supports a maximum of one E.164 number per gatekeeper-controlled H.323 client. If the gatekeeper field is populated, you cannot configure a second DN. If an H.323 client is configured for more than one DN, you cannot add the extra gatekeeper information to the database.
- The Gatekeeper routes call by using zone information when there is no zone prefix.

Configuration notes

Be aware of the following items for configuration purposes:

- You must ensure that gatekeeper is configured in Cisco Unified Communications Manager before an H.323 client can specify that gatekeeper in its configuration. The Gatekeeper field stays empty by default.
- Be sure to add the gatekeeper name, technology prefix, zone, and E.164 fields to the H.323 client configuration. You do not need to add Terminal Type. Default specifies the gateway type. If the gatekeeper is not chosen for the gatekeeper field during configuration of each of these fields, these fields cannot populate.
- Gatekeeper, zone, technology prefix fields, and E.164 information display under the Gatekeeper Information group on H.323 Client configuration.
- When an H.323 client uses the same gatekeeper, zone and technology prefix as those of another client, consider both clients in the same group. This group represents a single endpoint to the gatekeeper.
- You cannot use the same zone name for the H.323 client and trunk. A zone that an H.323 client uses must differ from the one that an H.323 trunk or a gatekeeper-controlled intercluster trunk uses.
- Ensure the service parameter, Send Product Id and Version ID, is set to True.
If an H.323 client is configured with an E.164 address and a gatekeeper, the database stores this information when the configuration is updated. This information gets loaded at boot time or when the device is reset.

**H.239-Extended video channels in H.323 call**

The extended video channels feature works via H.239 protocol and enables multiple video channel support. Cisco Unified Communications Manager supports negotiating an extended video channel using the H.239 protocol in direct point-to-point H.323 calls. This also includes calls across the H.323 intercluster trunk. Cisco Unified Communications Manager supports all H.239 associated support signals and commands that are specified in the H.239 recommendation.

The following sections describes characteristics which apply to the extended video channels feature.

**Support for third-party H.323 devices**

The extended video channel feature supports H.239 interoperability among third-party video endpoints and Cisco Unified Voice Conferencing. Cisco Unified Communications Manager allows an extended video channel to be used for presentation and live meeting transmission. This feature focuses on multiple video channel support via H.245 signaling. The following presentation applications provide basis for this multichannel support:

- Natural Presenter package by the third-party vendor Tandberg
- People + Content by the third-party vendor Polycom

Both Natural Presenter package and People + Content use the H.239 protocol to negotiate capabilities and define the roles of the additional video channels.

---

**Note**

Natural Presenter package by Tandberg and People + Content by Polycom only support H.239 for the presentation mode.

---

**Note**

Be aware that the presentation applications that are offered by Tandberg and Polycom are optional features. You must have one of these options and H.239 enabled in both caller and callee endpoints to negotiate second video channels or the call will be limited to a single video channel.

---

**H.323 devices invoke presentation feature**

Tandberg and Polycom video endpoints allow the user to share presentation materials from various components (for example, VCR, Projector, PC, and so on). The components can physically connect with the endpoints, and the PC can also run presentation applications that are provided by the vendor to transmit the presentation image. The source of presentation and the component connection with the video endpoint are irrelevant to the mechanism of establishing video channels by using H.239.

---

**Note**

For details on setting up presentation sources, see the video endpoint user guide.
When two H.239-enabled endpoints attempt to establish a video call, they declare their video capabilities for the main video channel for meeting participants and their extended video capabilities (H.239 capabilities) for the second video channel. The following contents comprise H.239 capability signals:

1. The endpoints send signals to indicate that the devices support H.239. They also send associated commands and indication signals for managing the second video channel. This enables both the endpoints to be aware that the call is capable of opening multiple video channels.

2. The endpoints send out one or more extended video codec capabilities to express video codec capabilities for second channels. The endpoint must specify the role of the second video channel. The defined role labels can be:
   - Live-video: This channel gets processed normally and is suitable for live video of people
   - Presentation: This channel relays a token-managed presentation that is distributed to the devices

After the capabilities have been exchanged, both endpoints immediately open two-way audio channels and the main video channels as in the traditional video calls.

**Opening second video channels**

Depending on the third-party endpoint implementation, the second video channel is handled differently among vendors.

**Natural Presenter Package by Tandberg**

Tandberg initiates the second video channel on demand. A Tandberg device does not open the second video channel immediately after the main video channel is established. The second channel gets opened when one of the callers (the presenter) specifies the source of the presentation and invokes a command to start the presentation.

When a Tandberg user decides to start sharing the presentation, Tandberg requests the other call party to open an extended video channel for receiving the presentation image; therefore, a Tandberg-Tandberg call has only one-way second video channel.

**People + Content by Polycom**

Unlike Tandberg, a Polycom video endpoint initiates the second video endpoint immediately as a part of the default mechanism, after both parties have confirmed that additional video channels can be supported.

**Note**

The channel established gets automatically if both parties support H.239 and have the extended video channel feature enabled. However, the additional channel does not show anything until one of the parties start to share presentation.

Polycom initiates a request for the second video channel to the other call party regardless of the usage of the second video channel; therefore, in a Polycom-Polycom call, two-way video channels get opened between the devices even if only one of them sends out presentation image/video.

This implementation ensures that both call parties have the second video channel ready for transmission when the call parties decide to take the token to present something. Although one of the two video channels remains idle (not sending anything), the Polycom device controls bandwidth to ensure load efficiency.
This difference in handling second video channels does not affect the implementation of H.239. Cisco Unified Communications Manager does not initiate any receiving channel request in an H.323-H.323 call. Cisco Unified Communications Manager simply relays all channel requests from one terminal to another.

Cisco Unified Communications Manager does not enforce two-way transmission for the second set of video channels because this does not represent a requirement in the H.239 protocol.

Call Admission Control (CAC) on second video channels

The following call admission control policies of Cisco Unified Communications Manager get applied to the second video channels:

Cisco Unified Communications Manager restricts the bandwidth usage by the second video channels on the basis of location configuration. When the second video channel is being established, Cisco Unified Communications Manager makes sure that enough video bandwidth stays available within the location pool and reserves bandwidth accordingly. If the required bandwidth is not available, Cisco Unified Communications Manager instructs the channel to reduce the available bandwidth to zero.

No change occurs in the region configuration or policies to support the second video channels.

Traditionally, Cisco Unified Communications Manager region policy has only supported a call with a single video channel and the total bandwidth usage of this call never gets larger than what the region configuration specifies.

If the administrator sets a finite region video bandwidth restriction for an H.239 call, Cisco Unified Communications Manager will violate the region policy because the region value will get used against the bandwidth that is requested for each video channel independently.

Example:

If the region video bandwidth is set to 384Kbps and the audio channel uses 64Kb/s, the maximum allowed bandwidth for each video channel will be (384Kb/s - 64Kb/s) = 320Kb/s.

i.e. the maximum bandwidth to be used by the H.239 call will be (audio bw + 2*(384 - audio bw)) = 704Kb/s, which goes beyond the 384Kb/s bandwidth that the region specifies.

You should consider relaxing both region and location bandwidth restrictions for H.239 calls, so the H.239 devices are allowed to re-adjust and balance load for both the video channels without Cisco Unified Communications Manager intervention.
Number of video channels allowed

Cisco Unified Communications Manager 8.5(1) supports only a maximum of two video channels due to the following reasons:

- Both Tandberg and Polycom only support two video channels, one of which is for main video, and the other is for presentation.
- H.239 only defines an Additional Media Channel (AMC) for H.320-based system to partition the traditional H.320 video channel for the purpose of presentation.

H.239 commands and indication messages

Command and Indication (C&I) messages get used for H.239 to manage tokens for the Presentation and Live roles and to permit devices to request release of video flow control to enable the operation of additional media channels. Cisco Unified Communications Manager supports all the C & I messages. Whenever Cisco Unified Communications Manager receives C&I messages, it relays them to the call party accordingly.

Be aware that the flow control release request and response messages can be used to request that the far end release flow control, so it allows an endpoint to send the indicated channel at the indicated bit rate.

Note

Be aware that the call party may or may not honor the request as is indicated by flow control release response.

The Presentation role token messages allow an H.239 device to acquire the token for presentation. The other call party may accept or reject the request. The presenter device sends out a token release message when it is no longer needed.

Topology and protocol interoperability limitation

Cisco Unified Communications Manager 8.5(1) supports only H.239 in H.323 to H.323 calls. Cisco Unified Communications Manager allows H.239 calls to be established across H.323 intercluster trunk or multiple nodes. If an H.239-enabled device attempts to make a call with a non-H323 end, the H.239 capabilities will get ignored and the call will get conducted like the traditional video calls that are supported by Cisco Unified Communications Manager.

Cisco Unified Communications Manager does not support a second video channel when a media termination point or transcoder is inserted into the call. If it happens, the call will fall back to normal video calls.

Midcall feature limitation

Cisco Unified Communications Manager supports opening second video channels only in direct H.323 to H.323 calls.

Caution

Do not attempt to invoke any midcall features such as call transfer or hold/resume operations. Doing so can lead to problems and the second video channel can get disconnected.
Skinny client control protocol video

Skinny Client Control Protocol video exhibits the following characteristics:

- If a phone that is running Skinny Client Control Protocol reports video capabilities, Cisco Unified Communications Manager automatically opens a video channel if the other end supports video.
- For Skinny Client Control Protocol video calls, system administration determines video call bandwidth by using regions. The system does not ask users for bit rate.

Skinny client control protocol video bridging

Video conferencing requires a Skinny Client Control Protocol video bridge. Skinny Client Control Protocol video bridging exhibits the following characteristics:

- Skinny Client Control Protocol video bridging requires the same setup as an audio bridge.
- Skinny Client Control Protocol video bridging supports a mix of audio and video in a conference.
- Media resource group lists determine whether an endpoint receives an audio or video bridge. That is, the media resource group list configuration of the user who sets up the conference determines whether the conference is a video conference or an audio-only conference.

Video over Wi-Fi

With a dual mode smart client running on a video-capable smart phone and registered to Cisco Unified Communications Manager, a video call can take place between the smart phone and another video capable end point over VoIP.

If a Cisco Dual Mode for iPhone (TCT) is video capable, it can call another video capable end point through the Cisco Unified Communications Manager over IP.

A video enable/disable toggle option is available on the device page of CCMAdmin. Additionally, mid-call features like Hold/Resume, conference, transfer with video are available.

MTP interactions and Limitations:

- A software MTP allocated in the call, does not support video streaming.
- A hardware multimedia MTP allocated allows video, with the condition that MTP allocated due to transcoder, TRP check on devices/trunks/gateways, video is not supported.
- When Unified Mobility requires the MTP for DTMF detection, video is available.
- MTP allocated due to transcoder, TRP check on devices/trunks/gateways, video will be available.

Video for SNR call

In Cisco Unified Communications Manager, if two endpoints including the remote destination are video capable, then mobility allows video streaming along with audio. The following example demonstrates this scenario:

1. Phone A (video capable) and Phone B are in cluster 1.
Phone C (video capable) is the remote destination shared line with Phone B is in cluster 2.
Phone A calls Phone B.
Phone C rings because of Single Number Reach.
If you pick up Phone C and both Phone A and Phone C are video capable, then a video call takes place.

**Limitations and Conditions**

- If in the entire call setup, Cisco Unified Communications Manager allocates a software MTP, then video streaming is not supported because MTP does not support video streaming.
- A hardware multimedia IOS MTP allocated in the call may result in video with certain conditions:
  - If the MTP is allocated because of MTP Required check on trunks and gateways, then video streaming does not occur.
  - If Unified Mobility requires MTP for DTMF detection, video is not available.
  - If MTP is allocated due to transcoder and a TRP check on devices, trunks, and gateways, video is available.

**SIP video**

SIP video supports the following video calls by using the SIP Signaling Interface (SSI):

- SIP to SIP
- SIP to H.323
- SIP to SCCP
- SIP intercluster trunk
- H.323 trunk
- Combination of SIP and H.323 trunk

SIP video calls also provide media control functions for video conferencing.

Cisco Unified Communications Manager video supports SIP, and both SIP trunks and lines support video signaling. SIP supports the H.261, H.263, H.263+, and H.264 video codecs (it does not support the wideband video codec that the VTA uses).

The Media Termination Point (MTP), which is used for RFC 2833, supports multiple logical channels within a session. A logical channel could exist for audio or video. To support video channels, the MTP uses pass-through mode. Video pass-through gets enabled if the MTP supports both pass-through and multiple logical channels. Not all MTP devices support multiple logical channels and pass-through mode.

**Configuring SIP devices for video calls**

Perform the following steps to enable video calls on SIP devices:
SIP Trunks

- On the Trunk Configuration window in Cisco Unified Communications Manager Administration, check the Retry Video Call as Audio check box if you want the call to use audio when the video connection is not available.
- Reset the trunk.

Cisco Unified IP Phone 9951 and 9971

- On the Phone Configuration window in Cisco Unified Communications Manager Administration, set the Cisco Camera and Video Capabilities product specific configuration to Enabled.
- Reset the phone.

For more information, see the Cisco Unified IP Phone 8961, 9951, 9971 User Guide for Cisco Unified Communications Manager (SIP).

Third-Party SIP Endpoints

- On the Phone Configuration window in Cisco Unified Communications Manager Administration, check the Retry Video Call as Audio check box if you want the call to use audio when the video connection is not available.
- Reset the endpoint.

Related Topics

Additional configuration for video calls, on page 570
Trunk interaction with H.323 client, on page 571
Configure video telephony, on page 543

Cisco video conference bridges

Cisco Unified Communications Manager supports a variety of solutions for video conferencing. The following video conference bridges support ad hoc and meet-me video conferencing:

- Cisco TelePresence MCU
- Cisco Unified MeetingPlace
- ISR G2 router video conference bridge

Cisco TelePresence MCU video conference bridge

Cisco TelePresence MCU is a set of hardware conference bridges for Cisco Unified Communications Manager. The Cisco TelePresence MCU is a high-definition (HD) multipoint video conferencing bridge. It delivers up to 1080p at 30 frames per second, full continuous presence for all conferences, full transcoding, and is ideal for mixed HD endpoint environments. The Cisco TelePresence MCU supports SIP as the signaling call control protocol. It has a built in Web Server that allows for complete configuration, control, and monitoring of the system and conferences. The Cisco TelePresence MCU provides XML management API over HTTP.
Cisco TelePresence MCU allows both ad hoc and meet-me voice and video conferencing. Each conference bridge can host several simultaneous, multiparty conferences. Cisco TelePresence MCU must be configured in Port Reservation mode.

Cisco Unified MeetingPlace video conference bridge

Cisco Unified MeetingPlace is a comprehensive collaboration solution that can be configured to act as a video conference bridge that supports both ad hoc and meet-me video conferencing. Cisco Unified MeetingPlace also integrates with Cisco WebEx to provide a variety of web conferencing and content-sharing solutions.

Cisco Unified MeetingPlace deployments vary in size and complexity. The solution may be housed on a single server, or on multiple servers. All Cisco Unified MeetingPlace deployments include an Application Server, which is installed on a Cisco MCS. The Application Server controls the media servers of the solution.

Video conferencing functionality is provided by the media server. The Cisco Unified MeetingPlace solution provides two media server options: an Express Media Server and a Hardware Media Server. The Express Media Server is a software-based media server that is installed on the Application Server, thereby allowing for a single-box deployment. The Hardware Media Server consists of audio and video blades installed on a separate Cisco 3500 series media server.

For web deployments, an optional web server may also be included.

Conferencing Capabilities

If Cisco Unified MeetingPlace is configured as a conference bridge, and the Express Media Server deployment is used, the conference bridge supports both ad-hoc and meet-me video conferencing. The Express Media Server supports both the H.263 and H.264/AVC video codecs, but transcoding between different codecs within a single meeting is not supported.

With the Express Media Server, the video mode, which specifies the display resolution, must be set before the conference begins. For ad-hoc conferencing, all ad-hoc meetings share a single system-wide setting. If you want legacy CIF endpoints to participate in ad hoc video conferences, then all ad-hoc meetings must be limited to CIF resolution of 352 x 288.

If the Hardware Media Server deployment is used, the conference bridge supports meet-me video conferencing only. Transcoding between video codecs is supported. Additionally, participants can record the audio and video portions of meetings.

The following table summarizes the main videoconferencing features available in Cisco Unified MeetingPlace. Please note that overall conferencing capacity depends on a variety of factors, including the configuration settings as well as the physical hardware. Overall capacity is highest for lower resolution video along with a low bandwidth audio codec, such as G.711. Using high-definition video or a high bandwidth audio codec will result in lower capacity.

For more detailed information on the capabilities of Cisco Unified MeetingPlace, refer to the Cisco Unified MeetingPlace product documentation.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Express Media Server</th>
<th>Hardware Media Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conferencing</td>
<td>Ad hoc and meet-me</td>
<td>Meet-me</td>
</tr>
<tr>
<td>Audio codecs</td>
<td>G.711</td>
<td>G.711</td>
</tr>
<tr>
<td></td>
<td>G.722</td>
<td>G.722</td>
</tr>
<tr>
<td></td>
<td>G.729a</td>
<td>G.729a</td>
</tr>
<tr>
<td></td>
<td></td>
<td>iLBC</td>
</tr>
<tr>
<td>Feature</td>
<td>Express Media Server</td>
<td>Hardware Media Server</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>------------------------------------------</td>
<td>---------------------------------------------</td>
</tr>
<tr>
<td>Video codecs</td>
<td>H.263</td>
<td>H.261</td>
</tr>
<tr>
<td></td>
<td>H.264/AVC</td>
<td>H.263</td>
</tr>
<tr>
<td></td>
<td></td>
<td>H.264/AVC</td>
</tr>
<tr>
<td>Recording</td>
<td>Cannot record the video</td>
<td>Can record both audio and video portion of meetings</td>
</tr>
<tr>
<td>Transcoding between H.264 and H.263/AVC</td>
<td>Not supported in same meeting, although both codecs are supported</td>
<td>Supported</td>
</tr>
<tr>
<td>Video resolution</td>
<td>Up to 1280x720</td>
<td>352 x 288</td>
</tr>
<tr>
<td>Total number of callers</td>
<td>Up to 1300 for audio</td>
<td>Up to 2000 for audio</td>
</tr>
<tr>
<td></td>
<td>Up to 650 for video</td>
<td>Up to 300 for video</td>
</tr>
<tr>
<td>Note</td>
<td>These numbers assume low-resolution video with the G.711 audio codec. Using a higher video resolution or a higher bandwidth audio codec will reduce the numbers</td>
<td></td>
</tr>
</tbody>
</table>

**ISR G2 Router video conference bridge**

Cisco Integrated Services Routers Generation 2 (ISR G2) can be enabled to act as IOS-based conference bridges that support ad hoc and meet-me audio and video conferencing. To enable conferencing, a PVDM3 DSP module must be installed on the ISR G2 router. The ISR G2 routers include the following series:

- Cisco 2900 series
- Cisco 3900 series

For ad hoc video conferencing, the ISR G2 router supports up to 8 participants. For meet-me video conferencing, support is provided for up to 16 participants. For video conferences, the resolution, bit rate and frame rates vary depending on which video format is used, but the ISRG2 routers can support a frame rate of up to 30 f/s, a stream bit rate up to 2 Mb/s and video resolution of up to 704 x 568 pixels. For a detailed breakdown of the codecs, frame rates, bit rates and video resolution for each video format, refer to the document, Configuring Video Conferences and Video Transcoding.

Within Cisco Unified Communications Manager, ISR G2 routers can be configured as one of three conference bridge types:

- Cisco IOS Homogeneous Video Conference Bridge—In a homogeneous video conference all the conference participants connect to a conference bridge with phones that support the same video format attributes. All the video phones support the same video format and the conference bridge sends the same data stream format to all the video participants.
- Cisco IOS Heterogeneous Video Conference Bridge—In a heterogenous video conference all the conference participants connect to the conference bridge with phones that use different video format...
attributes. Transcoding features are required from the DSP in order to convert the signal from one video format to another.

- Cisco IOS Guaranteed Audio Video Conference Bridge—In a guaranteed audio video conference the DSP resources for the audio conference bridge are reserved, but video service is not guaranteed. This may be necessary if DSP resources are limited. Callers on video phones may have video service if DSP resources are available at the start of the conference. Otherwise, the callers are connected to the conference as audio conference.

For more detailed information on video conferencing with ISR G2 routers, refer to the document Configuring Video Conferences and Video Transcoding.

Cisco TelePresence Video Communications Server

Cisco Unified Communications Manager can interoperate with a Cisco TelePresence Video Communications Server (VCS). To make the two systems compatible, you must configure a SIP normalization script on the SIP trunk that connects Cisco Unified Communications Manager to the Cisco VCS. The normalization script adjusts the SIP signaling so that the two products can communicate.

Cisco TelePresence Video Communication Server provides advanced telepresence and video conferencing call control for the Cisco TelePresence line of products. It enables any-to-any interoperability between all standards-compliant SIP and H.323 devices and offers three deployment options:

- Server Control
- Server Expressway
- Starter Pack Express

As a Server Control, Cisco TelePresence Video Communication Server provides advanced telepresence applications and session management to all standards-compliant telepresence endpoints, infrastructure, and management solutions. Cisco VCS Control provides Session Initiation Protocol (SIP) proxy and H.323 gatekeeper services.

As a Server Expressway, Cisco TelePresence Video Communication Server provides standards-based and secure firewall traversal for SIP and H.323 devices. Cisco VCS Expressway enables business-to-business communications, empowers remote and home-based workers, and allows service providers to provide video communications to customers.

In the Starter Pack Express deployment, Cisco TelePresence Video Communication Server provides an all-in-one solution targeted to customers who are deploying small to medium-sized Cisco TelePresence systems for the first time.

Configure interoperability with Cisco TelePresence Video Communications Server

To enable Cisco Unified Communications Manager to interoperate with a Cisco VCS, perform the following steps on the SIP trunk that connects Cisco Unified Communications Manager to Cisco VCS
Procedure

Step 1 In Cisco Unified Communications Manager Administration, choose **Device > Device Settings > Trunk.**

Step 2 Choose the SIP trunk that connects Cisco Unified Communications Manager to the Cisco VCS.

Step 3 In the SIP Profile drop-down list box, choose **Standard SIP Profile for VCS.**

Step 4 In the Normalization Script drop-down list box, choose **vcs-interop.**

Step 5 In the Normalization Script area, leave the Parameter Name and Parameter Value fields empty. If these fields are already populated, delete the contents of the field.

Video encryption

Cisco Unified Communications Manager supports encryption of audio, video, and other media streams so long as the individual endpoints involved in the communication also support encryption. Cisco Unified Communications Manager uses the Secure Real-Time Transport Protocol (SRTP) to encrypt the media streams. Some of the features include:

- Support for SIP and H.323 endpoints
- Support for encryption of main audio and video line while operating in Media Termination Point (MTP) passtrhru mode
- Support for multiple encryption methods
- Support for Session Description Protocol (SDP) crypto-suite session parameters in accordance with RFC 4568

To provide encrypted communications, encryption keys are exchanged between the endpoints and Cisco Unified Communications Manager during the SIP call setup. For this reason, the SIP signaling should be encrypted using TLS. During the initial call setup, the video endpoints exchange a list of encryption methods they support, select an encryption suite supported by both endpoints, and exchange encryption keys. If the endpoints cannot agree on a common encryption suite, the media streams are unencrypted and transported using the Real-Time Transport Protocol (RTP).

Note

If the individual endpoints do not support encryption, the communication will take place using RTP.

Encryption methods

Cisco Unified Communications Manager supports different encryption suites. The encryption method is identified using the Crypto-suite option in the SDP portion of the SIP message. The following table shows which SDP encryption suites are supported by Cisco Unified Communications Manager.
Table 51: Supported SDP Encryption Suites

<table>
<thead>
<tr>
<th>Encryption Standard</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AES_CM_128_HMAC_SHA1_80</td>
<td>128-bit encryption key and an 80-bit message authentication tag</td>
</tr>
<tr>
<td>AES_CM_128_HMAC_SHA1_32</td>
<td>128-bit encryption key and a 32-bit message authentication tag</td>
</tr>
<tr>
<td>F8_128_HMAC_SHA1_80</td>
<td>128-bit encryption key and an 80-bit message authentication tag</td>
</tr>
</tbody>
</table>

In addition to the above methods, Cisco Unified Communications Manager also supports DTLS encryption of media streams.

Negotiation of the encryption method

The selection of the encryption method to be used for an individual call is made according to which encryption suites are available on the individual endpoints themselves. If the endpoints cannot agree on an encryption method, then media is not be encrypted and is transported using RTP.

Cisco Unified Communications Manager uses the SIP Offer/Answer model to establish SIP sessions, as defined in RFC 3264. In this context, a calling device makes an Offer contained within the SDP fields in the body of a SIP message. The Offer typically defines the media characteristics supported by the device, including the encryption method that is supported by that device, as well as media streams, codecs, IP addresses, and ports to use.

The receiving device responds with an Answer in the SDP fields of its SIP response, with its own corresponding encryption suites, matching media streams, codecs, and the IP address and port on which to receive the media streams. Cisco Unified Communications Manager uses this Offer/Answer model to establish SIP sessions as defined in the key SIP standard, RFC 3261.

The operation of the SIP Offer/Answer model can differ depending on the features. The process is slightly different for Early Offer and Delayed Offer:

- In an Early Offer session, the called device selects the appropriate encryption suite. In this case, the calling device sends its preferred encryption suites in the original SIP invite message. The called device compares the list of encryption methods offered by the caller to its own list of available encryption methods, and selects the best option. Re-Invites will be handled the same as Early Offer.

- In a Delayed Offer session, the calling device includes a list of supported encryption methods. When it receives the initial invite, Cisco Unified Communications Manager forwards the INVITE on to the called device without the SDP portion that contains the encryption methods. The called device responds with its own list of encryption methods. Cisco Unified Communications Manager compares the two lists and selects an appropriate encryption method that is supported by both endpoints.

Limitations

Cisco Unified Communications Manager has the following limitations with video encryption:

- Cisco Unified Communications Manager does not provide support for the UNENCRYPTED_RTP SDP crypto-line parameter. The call is downgraded to RTP if no other SDP crypto-line parameters are present.
• If the SDP offer contains multiple keys, only the first key is used. The other keys are dropped and the call continues using only the first key.

**Supported protocols**

The following table shows which encryption methods are supported when specific signaling methods are used.

*Table 52: Encryption Support for Supported Protocols*

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP-SCCP</td>
<td>Video encryption is not supported over SCCP.</td>
</tr>
<tr>
<td>SIP-SIP using MTP/RSVP/TRP</td>
<td>Video encryption is supported. However, in MTP passthru mode only main audio and video lines are encrypted.</td>
</tr>
<tr>
<td>SIP-SIP over H.323 ICT</td>
<td>Video encryption is not supported over H.323 trunks. Only audio encryption is supported.</td>
</tr>
<tr>
<td>SIP-H.323</td>
<td>Video encryption is not supported for calls from SIP to H.323 endpoints.</td>
</tr>
<tr>
<td>H.323-H.323</td>
<td>Video encryption is supported using H.235.</td>
</tr>
</tbody>
</table>

**Endpoint support for the Binary Floor Control Protocol**

Cisco Unified Communications Manager 8.6(2) provides support for the Binary Floor Control Protocol (BFCP) for specific Cisco and third-party video endpoints. BFCP allows users to share a presentation within an ongoing video conversation.

The following example shows how presentation sharing using BFCP works:

An ongoing video conversation exists between two video phones. User A decides to show User B a slide presentation that is saved on a laptop. User A attaches the laptop to a Cisco EX90 video phone and presses the Present button on the phone. The SIP INVITE message gets initiated to the other phone, forming the invitation for a BFCP stream. After the BFCP session is negotiated, an additional stream is added to the audio and video streams. The BFCP stream allows User B to see the desktop on User A's laptop.

**BFCP Support on Cisco Video Endpoints**

For the following Cisco video endpoints, BFCP is enabled by default through the endpoint Qualification and Evaluation of device (QED) settings. Because BFCP is automatically enabled, Cisco Unified Communications Manager does not provide configuration options for these endpoints.

- Cisco E20
- Cisco TelePresence Codec C40
- Cisco TelePresence Codec C60
- Cisco TelePresence Codec C90
• Cisco TelePresence EX60
• Cisco TelePresence EX90
• Cisco TelePresence Quick Set C20
• Cisco TelePresence Profile 42 (C20)
• Cisco TelePresence Profile 42 (C60)
• Cisco TelePresence Profile 52 (C40)
• Cisco TelePresence Profile 52 Dual (C60)
• Cisco TelePresence Profile 65 (C60)
• Cisco TelePresence Profile 65 Dual (C90)
• Cisco TelePresence
• Cisco TelePresence 1000
• Cisco TelePresence 1100
• Cisco TelePresence 1300-47
• Cisco TelePresence 1300-65
• Cisco TelePresence 1310-65
• Cisco TelePresence 3000
• Cisco TelePresence 3200
• Cisco TelePresence 500-32
• Cisco TelePresence 500-37

**BFCP Support on Third-Party Phones**

For the following third-party video endpoints, BFCP is disabled by default, but support can be enabled in the Protocol Specific Information section of the Phone Configuration window:

• Generic Desktop Video Endpoint
• Generic Multiple Screen Room System
• Generic Single Screen Room System
• Third Party SIP Device (Advanced)

**Cisco Unified Communications Manager Administration Configuration Tips**

Presentation sharing using BFCP is supported only on full SIP networks. The entire network, including the endpoints and all the intermediary devices and trunks, must be SIP. BFCP must be enabled on all SIP trunks and lines.

To configure BFCP on SIP trunks, check the **Allow Presentation Sharing** using BFCP check box in the Trunk Specific Configuration section of the SIP Profile Configuration window.

To configure BFCP on SIP lines:

• For Cisco video endpoints that support BFCP, no configuration on the SIP line is required.
For third-party video endpoints that support BFCP, enable BFCP by checking the **Allow Presentation Sharing** using BFCP check box in the Protocol Specific Information section of the Phone Configuration window.

The following GUI changes were made for this feature:

- **Device Settings > SIP Profile**—The **Allow Presentation Sharing** using BFCP check box has been moved to the Trunk Specific Configuration section of the SIP Profile Configuration window.

- **Device Settings > Phone**—The **Allow Presentation Sharing** using BFCP check box has been added to the Protocol Specific Information section of the Phone Configuration window for the following third-party phones:
  - Generic Desktop Video Endpoint
  - Generic Multiple Screen Room System
  - Generic Single Screen Room System
  - Third-party SIP Device (Advanced)

**BFCP Negotiation in MTP Topologies**

A new version (15.2(2)T) of the IOS Media Terminating Point (MTP) router is now available which allows up to 16 media streams per session (previous release only allows up to three streams), this enables Cisco Unified Communications Manager to support BFCP and second video channels. A BFCP call normally requires at least four channels, which are audio, main video, second video and BFCP Control channel, to achieve video conferencing and also sharing presentations in the second video channel. If the call parties are capable of Far-End Camera Control (FECC), a fifth channel would need to be established.

If the MTP does not have enough media ports to support a BFCP session, the BFCP media lines are not negotiated when the call is established.

**Presentation sharing with the Binary Floor Control Protocol**

Cisco Unified Communications Manager supports presentation sharing within an ongoing video conversation using the Binary Floor Control Protocol (BFCP).

Cisco Unified Communications Manager aids in the negotiation of the BFCP stream by relaying SIP messages between the two endpoints until a BFCP session can be established. This negotiation involves establishing a floor, which is a temporary permission to access shared resources. The BFCP stream is a point-to-point stream between the endpoints. Cisco Unified Communications Manager is never the target of the BFCP stream.

As an example of how presentation sharing with BFCP works, you could have an ongoing video conversation between two SIP video phones. User A decides to show User B a slide presentation that is saved on a laptop. User A attaches the laptop to a Cisco EX90 video phone and presses the Present button on the phone. This sends to the other phone a SIP INVITE message containing the SDP parameters for the creation of a BFCP
stream. After the BFCP session is negotiated, an additional stream is added to the audio and video streams. The BFCP stream allows User B to see the desktop of User A’s laptop.

BFCP is supported only on SIP networks. The entire network, including all endpoints, intermediary devices and trunks, must be SIP. BFCP must be enabled on all SIP trunks and SIP lines.

---

**Note**

BFCP is not supported with IME trunks, so BFCP should be disabled for SIP profiles that are used for IME trunks.

The following network diagram displays the network topology that is used for BFCP. The Cisco Unified Communications Manager clusters are involved only in forwarding SIP messages between the devices. After the endpoints negotiate BFCP, the BFCP stream itself is a point-to-point stream between the devices.

The following figure provides an example of a BFCP-capable network. The network is fully SIP capable. The Cisco Unified Communications Manager cluster sits in the middle and relays SIP signaling between the endpoints. The BFCP stream as well as the audio and video streams, are point-to-point between the endpoints.

---

**Figure 49: Simple Video Network Using BFCP**

---

**BFCP configuration tips**

To enable BFCP in Cisco Unified Communications Manager, check the **Allow Presentation Sharing using BFCP** check box in the SIP Profile Configuration window. If the check box is unchecked, all BFCP offers will be rejected. By default, the check box is unchecked.

BFCP is supported only on full SIP networks. For presentation sharing to work, BFCP must be enabled for all SIP endpoints as well as all SIP lines and SIP trunks between the endpoints.
The following figure provides an example of a complex video network with multiple Cisco Unified Communications Manager clusters. BFCP must be enabled on all the trunks and lines connecting the devices. For this network, BFCP must be enabled on the four SIP trunks and two SIP lines that connect the endpoints.

**Figure 50: Video Network with Multiple Cisco Unified Communications Manager Clusters**

### BFCP limitations

Cisco Unified Communications Manager rejects the BFCP stream in the following scenarios:

- The **Allow Presentation Sharing using BFCP** check box on the **SIP Profile** page is unchecked for one of the SIP lines or trunks in the network.
- One endpoint offers BFCP, but the other does not.
- The SIP line or SIP trunk uses MTP, RSVP, Trusted Relay Point (TRP), or Transcoder. In these cases, BFCP is not supported.

**Note**

BFCP is supported in Cisco Unified CM Release 8.6 as long as the call does not require MTP. For Cisco Unified CM Release 9.0 or later BFCP in MTP call is supported if the MTP is allocated from IOS routers that run 15.2.(2) T.

- BFCP is supported only for SIP endpoints.

**Note**

BFCP is not supported when used between Cisco Unified Communications Manager and Cisco TelePresence MCU.

### Supported features with BFCP

The following table highlights how some of the common features are handled while a BFCP presentation is ongoing:
Table 53: Supported Features with BFCP

<table>
<thead>
<tr>
<th>Mid-call Feature</th>
<th>Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hold and Resume</td>
<td>The Hold and Resume feature is fully supported when using a BFCP-capable endpoint, whether the endpoint is currently in a BFCP presentation or not. However, the user may have to reenable the presentation following the Resume operation.</td>
</tr>
<tr>
<td>Transfer</td>
<td>The Transfer feature is fully supported when using a BFCP-capable endpoint, whether the endpoint is currently in a BFCP presentation or not. However, the user may have to reenable the Presentation following the Transfer operation.</td>
</tr>
<tr>
<td>Conference (non-BFCP conference controller)</td>
<td>BFCP media line and presentation video are not supported when a BFCP-capable conference controller is used. However, the main video streams are supported. If two BFCP-capable endpoints enter into a conference with a non-BFCP conference controller, the main video is enabled throughout the conference, but the BFCP media and presentation video are disabled.</td>
</tr>
</tbody>
</table>

Bandwidth management

Bandwidth allocations for audio and video calls are managed through the call admission control that regions and locations provide in Cisco Unified Communications Manager Administration.

The amount of bandwidth available for a specific call must be able to manage the combination of all media streams that are associated with the session, including voice, video, signaling, and any extra media, such as a BFCP presentation. Cisco Unified Communications Manager contains features able to manage bandwidth.

Call Admission Control

Call admission control enables you to control the audio and video quality of calls over a wide-area (IP WAN) link by limiting the number of calls that are allowed on that link at the same time. For example, you can use call admission control to regulate the voice quality on a 56-kb/s frame relay line that connects your main campus and a remote site.

Call admission control determines whether the caller has the right to call the requested number as well as verifying if there is sufficient bandwidth available to complete a call. Call Admission Control can reject calls due to insufficient bandwidth.

In Cisco Unified Communications Manager, locations-based call admission control works in conjunction with regions to define the characteristics of a network link. Regions and locations work in the following manner:

- Regions allow the bandwidth of video calls to be set. Regions define the maximum bit rate for each call, and hence, the type of codec, that is used on the link (and therefore, the amount of bandwidth that is used per call). For more information about regions, see Regions, on page 37.
- Locations define the amount of total bandwidth available for all calls on that link. When a call is made on a link the regional value for that call must be subtracted from the total bandwidth allowed for that link. For more information about locations, see Locations, on page 68.
For more information about call admission control, see Call admission control, on page 65.

Session level bandwidth modifiers

Cisco Unified Communications Manager provides location call admission control support for handling session level bandwidth modifiers. Session level bandwidth modifiers are communicated as part of the parameters in the SDP portion of the initial SIP signaling. These parameters indicate the maximum amount of bandwidth each endpoint will support for that type of call. These parameters are used, along with regions and locations settings, to set the bandwidth for each call.

During the initial call setup, both parties communicate to Cisco Unified Communications Manager their maximum allowed bandwidth for the call. Cisco Unified Communications Manager passes this communication to the other endpoint, but if the bandwidth that is specified by the endpoint is greater than the region setting, Cisco Unified Communications Manager replaces the value with the region bandwidth value.

Cisco Unified Communications Manager uses the following rules to determine the amount of bandwidth to allocate to a specific call:

• When Cisco Unified Communications Manager receives an Offer or Answer from an endpoint, it checks whether there is a session level bandwidth modifier in the SDP:
  ◦ If there is a session level bandwidth modifier, Cisco Unified Communications Manager retrieves the bandwidth value from the modifier. If there is more than one modifier type, it retrieves the modifier in the following order of preference: Transport Independent Application Specific (TIAS), Application Specific (AS), Conference Total (CT).
  ◦ If there is no session level bandwidth modifier, Cisco Unified Communications Manager retrieves the bandwidth value from the sum of the media level bandwidth modifiers. However, if there is BFCP or FECC in the call, it uses the TIAS value from the main media line.

• The allocated bandwidth is the maximum of what the two endpoints support up to the maximum value of the Region setting. The allocated bandwidth cannot exceed the region setting.

Cisco Unified Communications Manager uses the following logic when communicating with endpoints:

• When generating an Answer, Early Offer or Re-Invite Offer to an endpoint that contains more than one session level bandwidth modifier type (TIAS, AS, CT), Cisco Unified Communications Manager uses the same bandwidth value for each.

• When generating an answer, Cisco Unified Communications Manager uses the same session level bandwidth modifier type (TIAS, CT, AS) that was received in the initial offer.

• For backward compatibility with older versions of Tandberg endpoints (such as MXP 1700), Cisco Unified Communications Manager suppresses the Session Level Bandwidth Modifier when a video call is put on hold and music on hold (MOH) is inserted.

RSVP

RSVP supports SCCP and SIP video calls. Configure RSVP policy for call admission control by using the Location Configuration window in Cisco Unified Communications Manager Administration.

Related Topics

   Resource Reservation Protocol, on page 79
Alternate routing

If an endpoint cannot obtain the bandwidth that it needs for a video call, a video call retries as an audio call for the default behavior. To use route/hunt lists or Automated Alternate Routing (AAR) groups to try different paths for such video calls, uncheck the Retry Video Call as Audio setting in the configuration settings for applicable gateways, trunks, and phones.

Related Topics

Resource Reservation Protocol, on page 79

DSCP marking

Differentiated Services Code Point (DSCP) packet marking, which is used to specify the class of service for each packet, includes the following characteristics:

- Audio streams in audio-only calls default to EF.
- Video streams and associated audio streams in video calls default to AF41.
- You can change these defaults through the use of a service parameter. The following service parameter settings affect DSCP packet marking:
  - DSCP for Audio Calls (for media [RTP] streams)
  - DSCP for Video Calls (for media [RTP] streams)
  - DSCP for Audio Calls when RSVP Fails
  - DSCP for Video Calls when RSVP Fails
  - DSCP for ICCP Protocol Links

Phone configuration for video calls

The following setting for video-enabled devices affects video calls:

- Retry Video Call as Audio-By default, this check box remains checked. Thus, if an endpoint (phone, gateway, trunk) cannot obtain the bandwidth that it needs for a video call, call control retries the call as an audio call. This setting applies to the destination devices of video calls.
- Video Capabilities Enabled/disabled-This drop-down list box turns video capabilities on and off.

Related Topics

Configure video telephony, on page 543

Additional configuration for video calls

The following configuration considerations also affect the ability to make video calls in Cisco Unified Communications Manager:

- Trunk interaction with the H.323 client
- Call routing considerations
• Resetting gateway timer parameters

Related Topics
Configuring SIP devices for video calls, on page 556

Trunk interaction with H.323 client
Trunk interaction with the H.323 Client for video calls functions identically to interaction functions for audio calls. See the Trunks and gatekeepers in Cisco Unified Communications Manager, on page 451.

Related Topics
Configuring SIP devices for video calls, on page 556

Call routing for video calls
Call routing for video calls functions identically to call routing for audio calls.

Gateway timer parameter
For some bonding calls through the H.323/H.320 gateway, the gateway requires a longer time to exchange the H.323 TCS message. If the time required is greater than the timer setting for several Cisco CallManager service parameters, Cisco Unified Communications Manager will drop the call.

If the default Cisco Unified Communications Manager gateway timer values appear to be too short, Cisco Unified Communications Manager drops the call before completion of the call connection. Cisco recommends increasing the following service parameter timers values to avoid call failure:

• H245TCSTimeout=25
• Media Exchange Interface CapabilityTimer=25
• Media Exchange Timer=25

Conference control for video conferencing
Cisco Unified Communications Manager supports the following conference controls capabilities:

• Roster/Attendee List
• Drop Participant
• Terminate Conference
• Show Conference Chairperson/Controller
• Continuous Presence

Cisco Unified Communications Manager also supports the following video conference capabilities for Skinny Client Control Protocol phones:

• Display controls for video conferences. The Skinny Client Control Protocol phones can choose to use the continuous presence or voice-activated mode to view the video conference. When a mode is chosen,
a message gets sent to the bridge to indicate which mode to use on the video channel. Switching between modes does not require renegotiation of media.

- Display participant information such as the user name in the video stream. The system can use the participant information for other conferencing features such as roster.

**Video and interoperability**

Cisco Unified Communications Manager 8.5 supports native or direct interoperability between Cisco video endpoints and 3rd party video endpoints such as Polycom. This means that Cisco Unified Communications Manager does not require a media gateway or conference bridge, such as Cisco Unified Video Conferencing (CUVC), for a simple point-to-point call between the supported endpoints.

**Protocols and deployments**

Video and interoperability support the following protocols:

- SIP to SIP
- H323 to H323
- SIP to SIP Intercluster trunk (ICT) to SIP
- H323 to H323 ICT to H323
- SIP to H323 with or without ICT

For more information about limitations and special considerations of this features, see the Limitations, on page 573.

Video and interoperability support the following deployments:

- High-Definition interoperability for point-to-point calls
- Locations-based call admission control (CAC) only
- Presentation sharing and secure interop between TelePresence and third-party endpoints that support the Telepresence Interop Protocol (TIP)
- Multipoint calls involving Cisco TelePresence System (CTS), Cisco Unified Communications Manager, and third-party endpoints use Media transcoding Engine (MXE) and Cisco Unified Video Conferencing (CUVA)

**Cisco and third-party endpoints supported**

Video and interoperability support the following endpoints:

- Cisco-certified third-party video endpoints
- Cisco E20 (Tandberg E20)
- Cisco Unified Clients Services Framework (CSF) based clients, such as Cisco Unified Communication interface for Microsoft Office Communicator (CUCiMOC) or CUCiConnect (for example, Cisco WebEx)
- Cisco Unified Video Advantage (CUVA)
- Cisco Unified Personal Communicator (CUPC)
• Cisco Unified IP Phone 7985
• Cisco Unified IP Phone 9951 and 9971
• Cisco Unified IP Phone 8961 (requires CUVA)
• MeetingPlace Conference bridges, such as MP Hardware Media Switch (HMS) or Software Media Switch (SMS)

To find a Cisco-certified third-party device, go the following URL:
http://developer.cisco.com/web/partner/search

Perform the following steps:

1. Sign in to the Cisco Developer Network (CDN) (if applicable)
2. From the CDN main window, click the Technology Partners tab.
3. Click the Partner Search tab.
4. In the search box, enter the name of a 3rd party company (within all technologies) (for example, Polycom).
5. When the 3rd party company information displays, click the applicable links for more information.

Third-party devices get configured in Cisco Unified Communications Manager Administration, Phone Configuration. For the list of supported device types and licensing requirements, see Third-party SIP endpoints, on page 479.

Limitations

The following limitations apply:

• Advanced presentation sharing and security interoperability is supported only between two TelePresence Interop Protocol (TIP) capable endpoints.
• H239 presentation sharing and H235 security are supported only between two H323 endpoints.
• For ensure optimal resolution between the two endpoints, the protocol on the endpoints and the trunk should be identical; for example, SIP point-to-point endpoints connected by a SIP trunk.
• Locations-based CAC only for interoperability with TelePresence
• Ad hoc and Meet-Me conferencing support CUVC and MeetingPlace software media servers. Because the conferencing bridges support SCCP and the endpoints support SIP or H323, resolution may be limited to standard definition.
• Cisco Intercompany Media Engine (IME) is not supported between Cisco Unified Communications Manager endpoints and Telepresence.

Internet Protocol Version 6 (IPv6)

Cisco Unified Communications Manager Release 9.0 does not support video IPv6 calls. Video always uses IPv4. Video is disabled for any dual-stack or IPv6 audio device that is associated with Cisco Unified Video Advantage.
Far End Camera Control protocol support

The Far End Camera Control (FECC) protocol allows you to control a remote camera. Within video calls, FECC allows the party at one end of the call to control the camera at the far end. This control can include panning the camera from one side to the other, tilting the camera, or zooming in and out. For video conferences that use multiple cameras, FECC can be used to switch from one camera to another.

Cisco Unified Communications Manager supports the FECC protocol for video endpoints that are FECC-capable. Cisco Unified Communications Manager supports FECC for SIP-SIP calls or H.323-H.323 calls, but does not support FECC for SIP-H.323 calls. To support FECC, Cisco Unified Communications Manager sets the application media channel through SIP or H.323 signaling. After the media channel is established, the individual endpoints can communicate the FECC signaling.

Note
Prior to Cisco Unified CM Release 9.0, if a Media Terminating Point (MTP) was present in a SIP-SIP call, FECC was not available. For Cisco Unified CM Release 9.0, if there is an MTP (version 15.2(2)T or later) present in a SIP-SIP call, and there are five channels available for the call, then FECC can be enabled.

Video telephony and Cisco Unified Serviceability

Cisco Unified Serviceability tracks video calls and conferences by updating performance monitoring counters, video bridge counters, and call detail records (CDRs).

Performance monitoring counters

Video telephony events cause updates to the following Cisco Unified Serviceability performance monitoring counters:

- Cisco Unified Communications Manager
  - VideoCallsActive
  - VideoCallsCompleted
  - VideoOutOfResources

- Cisco H.323
  - VideoCallsActive
  - VideoCallsCompleted

- Cisco Locations
  - VideoBandwidthAvailable
  - VideoBandwidthMaximum
  - VideoOutOfResources
  - VideoCurrentAvailableBandwidth
• Cisco Gatekeeper
  ◦ VideoOutOfResources

• Cisco SIP
  ◦ VideoCallsCompleted
  ◦ VideoCallsActive

See the Cisco Unified Serviceability Administration Guide for details.

**Video bridge counters**

Video conference events cause updates to these Cisco video conference bridge performance monitoring counters:

• ConferencesActive
• ConferencesAvailable
• ConferencesCompleted
• ConferencesTotal
• OutOfConferences
• OutOfResources
• ResourceActive
• ResourceAvailable
• ResourceTotal

These counters also display in the Cisco Unified Communications Manager object with the VCB prefix.

**Call Detail Records**

Video telephony events cause updates to Call Detail Records (CDRs) in Cisco Unified Serviceability. These CDRs include the following information:

• IP address and port for video channels
• Codec: H.261, H.263, H.264, Cisco VT Camera wideband video
• Call bandwidth
• Resolution: QCIF, CIF, SQCIF, 4CIF, 16CIF, or Custom Picture Format

Cisco Unified Communications Manager also stores CDRs for midcall video and supports the following call scenarios:

• Skinny Client Control Protocol to Skinny Client Control Protocol calls
• Skinny Client Control Protocol to Skinny Client Control Protocol calls across an intercluster trunk (ICT)
Note  CDR gets added when video is added mid-call, but CDR entry does not get removed as part of midcall video removal (for example, Cisco Video Telephony Advantage gets turned off).
CHAPTER 45

Computer Telephony Integration

This chapter provides information about Computer telephony integration (CTI) which enables you to leverage computer-processing functions while making, receiving, and managing telephone calls. CTI applications allow you to perform such tasks as retrieving customer information from a database on the basis of information that caller ID provides. CTI applications can also enable you to use information that an interactive voice response (IVR) system captures, so the call can be routed to the appropriate customer service representative or so the information is provided to the individual who is receiving the call.

- Configure CTI, page 577
- Computer Telephony Integration applications, page 578
- CTIManager, page 579
- Media Termination Points, page 580
- CTI-controlled devices, page 580
- User management and CTI controlled devices, page 582
- Applications that monitor and control all CTI-controllable devices, page 583
- IPv6 and CTI, page 584
- Dependency records, page 584
- CTI redundancy, page 584

Configure CTI

Computer telephony integration (CTI) enables you to leverage computer-processing functions while making, receiving, and managing telephone calls. CTI applications allow you to perform such tasks as retrieving customer information from a database on the basis of information that caller ID provides. CTI applications can also enable you to use information that an interactive voice response (IVR) system captures, so the call can be routed to the appropriate customer service representative or so the information is provided to the individual who is receiving the call.

For a description of Cisco CTI applications, see the Computer Telephony Integration applications, on page 578.

To configure Cisco Unified Communications Manager for CTI applications follow these steps.
To make the CTI application secure, configure authentication and encryption for CTI.

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Configure the appropriate CTI Manager and Cisco Call Manager service parameters.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Add and configure an IP phone, CTI route points, or ports for each CTI application.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Configure the directory number for the CTI device.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Associate all devices that the application will use with the appropriate Cisco Unified Communications Manager group (via the device pool).</td>
</tr>
<tr>
<td>Step 5</td>
<td>Configure the end users and application users that will use CTI applications. Add the device that is used for CTI applications (for example, IP phone, CTI port) to the Controlled Devices list that is on the End User and Application Users Configuration window.</td>
</tr>
</tbody>
</table>
| Step 6 | Add the end users and application users to the Standard CTI Enabled user group.  
**Note** Ensure all CTI users are in the Standard CTI Enabled user group, but they may also be in other CTI user groups. |
| Step 7 | Activate the CTI Manager service on the appropriate servers, if not already activated. |
| Step 8 | Install and configure your applications. |
| Step 9 | Restart application engine (if required). |

### Computer Telephony Integration applications

The following list contains descriptions of some Cisco CTI applications that are available:

- **Cisco IP Communicator**—Cisco IP Communicator, a desktop application, turns your computer into a full-feature telephone with the added advantages of call tracking, desktop collaboration, and one-click dialing from online directories. You can also use Cisco IP Communicator in tandem with a Cisco Unified IP Phone to place, receive, and control calls from your desktop PC. All features function in both modes of operation.

- **Cisco Unified Communications Manager Auto-Attendant**—The Cisco Unified Communications Manager Auto-Attendant application works with Cisco Unified Communications Manager to receive calls on specific telephone extensions and to allow the caller to choose an appropriate extension.

- **Cisco Web Dialer**—Cisco Web Dialer, which is installed on a Cisco Unified Communications Manager server and is used in conjunction with Cisco Unified Communications Manager, allows Cisco Unified IP Phone users to make calls from web and desktop applications.

- **Cisco Unified Communications Manager Assistant**—The Cisco Unified Communications Manager Assistant feature enables managers and their assistants to work together more effectively. The feature comprises a call-routing service, enhancements to phone capabilities for the manager and the assistant, and assistant console interfaces that are primarily used by the assistant.
To determine which Cisco Unified Communications Manager CTI applications support SIP IP phones, see the application-specific documentation. For more information about Cisco SIP support, see Session Initiation Protocol, on page 397.

CTIManager

A program called CTIManager includes the CTI components that interface with the applications that are separated out of Cisco Unified Communications Manager. The CTIManager service communicates with Cisco Unified Communications Manager by using the Cisco Unified Communications Manager communication framework, System Distribution Layer (SDL). Installation of the CTIManager program occurs on the Cisco Unified Communications Manager server during the Cisco Unified Communications Manager installation. Only one CTIManager can exist on an individual server. An application (JTAPI/TAPI) can have simultaneous connections to multiple CTIManagers; however, an application can use only one connection at a time to open a device with media termination. See the following figure.

Figure 51: Cisco Unified Communications Manager Components That Are Used to Provide CTI Services to Applications

CTIManager provides two advanced, clusterwide service parameters that are used in conjunction with the CTI Super Provider capability:

- Maximum Devices Per Provider-This parameter specifies the maximum number of devices that a single CTI application can open. The default specifies 2000 devices.
- Maximum Devices Per Node-This parameter specifies the maximum number of devices that all CTI applications can open on any CTIManager node in the Cisco Unified Communications Manager system. The default specifies 800 devices.

If the configured limits are exceeded, CTI generates alarms, but the applications continue to operate with the extra devices. For more information on CTI Super Provider, see the User management and CTI controlled devices, on page 582.
Media Termination Points

CTI applications can terminate media on CTI ports and CTI route points in the following ways:

- **Static IP address and port number**—Specify the media IP address and port number when the device gets opened. In this case, the media always terminates at the same IP address and port for all calls that are on that device. Only one application can terminate the media in this way.

- **Dynamic IP address or port number**—Specify the media IP address or port number on a per-call basis. For each call that requires a media termination, notification gets sent to the application that requests the media termination information. The application then must send the IP address or port number back, so the media can go through. You can specify only the IP address or port number on a per-call basis. The capabilities of the device still get specified statically when the device is opened. With dynamic media termination, multiple applications can open a device (CTI port or route point) for media termination as long as the capabilities that each application specifies stay the same.

CTI-controlled devices

The following CTI-controlled device types exist:

- Cisco Unified IP Phones (SCCP and SIP)

  **Note**  
  CTI applications support only some phones that run SIP; for example, it does not support the Cisco Unified IP Phone 7940 and 7960.

- CTI ports
- CTI route points

  **Note**  
  If a directory number (DN) is a member of a line group or hunt list, any device (CTI port, CTI route point, phone that is running SCCP, or phone that is running SIP) that uses that DN should not be associated with a CTI user.

  **Note**  
  CTI devices do not support the multicast Music On Hold feature. If a CTI device is configured with a multicast MOH device in the media resource group list of the CTI device, call control issues may result. CTI devices do not support multicast media streaming.

Cisco Unified IP Phones

CTI-controlled Cisco Unified IP Phones comprise phones that are running SCCP that a CTI application can control. CTI supports SIP on the Cisco Unified IP Phones (7911, 7941, 7961, 7970, and 7971) from the CTI interfaces JTAPI and TAPI, with some limitations. CTI applications control and monitor phones that are running SIP in the same manner as CTI-controlled/monitored phones that are running SCCP.
For phones that are running SCCP, outbound dialing supports en bloc (the phone collects all digits before passing them to Cisco Unified Communications Manager for routing) or digit-by-digit collection. If dialing is done digit-by-digit, a CTI dialing call state notification gets sent to the phone when it goes off hook and the first digit is pressed for an outgoing call. For en bloc outbound dialing, the dialing call state notification gets delayed until the phone collects all the digits and sends them to Cisco Unified Communications Manager for routing.

For phones that are running SIP, en bloc dialing always gets used even if the user first goes off hook before dialing digits; the phone will wait until all the digits are collected before sending the digits to Cisco Unified Communications Manager. This means that the dialing call state notification will only get generated after enough digits are pressed on the phone to match one of the configured dialing patterns. In all cases, the dialing state notifications will always get generated prior to the call being routed to the destination (as is the case with phones that are running SCCP).

Phones that are running SIP control when and how long to play reorder tone. When a phone that is running SIP receives a request to play reorder tone, it releases the resources from Cisco Unified Communications Manager and plays reorder tone. Therefore, the call appears to be idle to a CTI application regardless of when reorder tone is played on the phone. In these scenarios, applications can receive and initiate calls from the phone regardless whether reorder tone plays on the phone. Because resources have been released on Cisco Unified Communications Manager, the call does not count against the busy trigger and maximum number of call counters (that are configured on the Directory Number Configuration window).

Cisco Unified IP Phones with SIP that are configured to use UDP as the transport mode (instead of TCP) do not support the device data pass-through functionality; for example, the Quality Reporting Tool (QRT) requires the data pass-through functionality, so it cannot be used with IP phones that are configured with UDP.

**CTI Ports**

CTI ports as virtual devices can have one or more virtual lines, and software-based Cisco Unified Communications Manager applications such as Cisco IP Softphone, Cisco Unified Communications Manager Auto-Attendant, and Cisco Unified IP Interactive Voice Response (IVR) use them. You configure CTI ports by using the same Cisco Unified Communications Manager Administration windows as you use to configure phones. For first-party call control, you must add a CTI port for each active voice line.

**CTI Route Point**

A CTI route point virtual device can receive multiple, simultaneous calls for application-controlled redirection. You can configure one or more lines on a CTI route point that users can call to access the application. Applications can answer calls at a route point and can also redirect calls to a CTI port or IP phone. When a CTI application requests to redirect a call by using the Redirect API, Cisco Unified Communications Manager uses the configuration for the line/device calling search space for the redirected party.

Route points can receive multiple, simultaneous calls; therefore, applications that want to terminate media for calls at route points must specify the media and port for the call on a per-call basis. CTI route points support the following features:

- Answer a call
- Make and receive multiple active calls
- Redirect a call
• Hold a call
• Unhold a call
• Drop a call

When a call arrives at a route point, the application must handle (accept, answer, redirect) it within a specified time. To configure the time that is allowed to answer a call, use the Cisco CallManager CTI New Call Accept Timer service parameter. Use the Directory Number Configuration window in Cisco Unified Communications Manager Administration to configure the number of simultaneous active calls on the route point.

**Note**

If you are planning to use a TAPI application to control CTI port devices by using the Cisco CallManager Telephony Service Provider (TSP), you may only configure one line per CTI port device.

Applications that are identified as users can control CTI devices. When users have control of a device, they can control certain settings for that device, such as answer the call and call forwarding.

CTI devices (CTI ports, CTI route points) must associate with device pools that contain the list of eligible Cisco Unified Communications Managers for those devices.

The maximum number of CTI-controlled devices per node varies by server class as follows:

• MCS-7825 and MCS-7835 servers support up to 800 CTI-controlled devices per node.
• MCS-7845 servers support up to 2500 CTI-controlled devices per node.

When a CTI device fails (during a Cisco Unified Communications Manager failure, for example), Cisco Unified Communications Manager maintains media streams that are already connected between devices (for devices that support this feature). Cisco Unified Communications Manager drops calls that are in the process of being set up or modified (transfer, conference, redirect, and so on).

## User management and CTI controlled devices

To allow a CTI application to control or monitor devices, ensure the devices are assigned to the end user or application user that is associated with the CTI application. This gets done by using the End User or Application User Configuration windows in Cisco Unified Communications Manager Administration. From the Device Association pane of the User Configuration window, an administrator associates the desired devices to the Controlled Devices list.

To allow CTI applications access to certain CTI capabilities, ensure the end user or application user that is associated with the application are added to one or more of the following CTI-related user groups:

• Standard CTI Allow Call Monitoring-This user group allows an application to monitor calls.
• Standard CTI Allow Call Park Monitoring-This user group allows an application to receive notification when calls are parked/unparked to all Call Park directory numbers.
• Standard CTI Allow Call Recording-This user group allows an application to record calls.
• Standard CTI Allow Calling Number Modification-This user group allows an application to modify the calling party number in supported CTI applications.
• Standard CTI Allow Control of All Devices-This user group allows an application to control or monitor any CTI-controllable device in the system.
• Standard CTI Allow Reception of SRTP Key Material-This user group allows an application to receive information that is necessary to decrypt encrypted media streams. This group typically gets used for recording and monitoring purposes.

• Standard CTI Enabled-This user group, which is required for all CTI applications, allows an application to connect to Cisco Unified Communications Manager to access CTI functionality.

• Standard CTI Secure Connection-Inclusion into this group will require that the application have a secure (TLS) CTI connection to Cisco Unified Communications Manager if the Cisco Unified Communications Manager cluster security is enabled.

Note
The CTI application must support the specified user group to which it gets assigned.

Note
Cisco recommends that users who are associated with the Standard CTI Allow Control of All Devices user group also be associated with the Standard CTI Secure Connection user group.

Applications that monitor and control all CTI-controllable devices

By adding an application user to the user group, Standard CTI Allow Control of All Devices, a CTI application can control any CTI-controllable devices that are configured in the Cisco Unified Communications Manager system. These applications sometimes get referred to as super provider applications. CTI super provider application dynamically associates/disassociates devices to/from an application control list, so this list/set of devices could be a variable list/set.

The system administrator configures the CTI super provider capability by adding the application user or end user to the Standard CTI Allow Control of All Devices user group. The administrator uses the User Groups Configuration window in Cisco Unified Communications Manager Administration to add users to user groups.

For information about CTI-controllable devices, see the CTI-controlled devices, on page 580.

All CTI applications with super provider capability exercise control over any CTI-controllable devices in the system. If an application needs to know only the status of a device, it opens the device and gets the status. Because CTI super provider controls any device, you cannot exclude any device from CTI super provider control. CTI system limits determine the maximum number of devices that a CTI application can control. See the CTIManager, on page 579 for a description of CTI maximum limits. If the limits are exceeded, CTI generates alarms.

If a CTI application monitors a call park number, you must add the application to the Standard CTI Allow Call Park Monitoring user group.

If a CTI application monitors calls, you must add the application to the Standard CTI Allow Call Monitoring user group. If the CTI application records calls, you must add the application to the Standard CTI Allow Call Recording user group.

Tip
To calculate the number of CTI monitored lines in a system, use the following formula:
number of pilot point DN's + (number of clients open * number of directory numbers per phone) + (number of parked directory numbers * number of open clients) = CTI Monitored Lines

IPv6 and CTI

Computer Telephony Integration (CTI) provides IP address information through the JTAPI and TAPI interfaces, which can support IPv4 and IPv6 addresses. To support IPv6, applications need to use a JTAPI / TAPI client interface version that supports IPv6.

Dependency records

To find the directory numbers that a specific CTI route point is using, choose Dependency Records from the Related Links drop-down list box that is provided on the Cisco Unified Communications Manager Administration CTI Route Point Configuration and CTI Port Configuration windows. The Dependency Records Summary window displays information about directory numbers that are using the route point. To find out more information about the directory number, click the directory number, and the Dependency Records Details window displays. If the dependency records are not enabled for the system, the dependency records summary window displays a message.

CTI redundancy

Cisco does not support redundancy for Cisco Unified Communications Manager Business Edition 5000 systems. CTI provides recovery of failure conditions that result from a failed Cisco Unified Communications Manager node within a cluster and failure of a CTIManager. This section describes the failover and fallback capabilities of the following components:

- Cisco Unified Communications Manager
- CTIManager
- Applications (TAPI/JTAPI)

Cisco Unified Communications Manager

When a Cisco Unified Communications Manager node in a cluster fails, the CTIManager recovers the affected CTI ports and route points by reopening these devices on another Cisco Unified Communications Manager node. If an application has a phone device open, the CTIManager also reopens the phone when the phone fails over to a different Cisco Unified Communications Manager. If the Cisco Unified IP Phone does not fail over to a different Cisco Unified Communications Manager, the CTIManager cannot open the phone or a line on the phone. The CTIManager uses the Cisco Unified Communications Manager group that is assigned to the device pool to determine which Cisco Unified Communications Manager to use to recover the CTI devices and phones that the applications opened.

When the CTIManager initially detects the Cisco Unified Communications Manager failure, it notifies the application (JTAPI/TAPI) that the devices on that Cisco Unified Communications Manager went out of service. If no other Cisco Unified Communications Manager in the group is available, the devices remain out
of service. When those devices successfully rehome to another Cisco Unified Communications Manager, the CTIManager notifies the application that the devices are back in service.

When a failed Cisco Unified Communications Manager node comes back in service, the CTIManager rehomes the affected CTI ports/route points to their original Cisco Unified Communications Manager. The rehoming process starts when calls are no longer being processed or active on the affected device. Because devices cannot be rehomed while calls are being processed or active, the rehoming process may not occur for a long time, especially for route points that can handle many simultaneous calls.

If none of the Cisco Unified Communications Managers in the Cisco Unified Communications Manager group is available, the CTIManager waits until a Cisco Unified Communications Manager comes into service and tries to open the CTI device again. If for some reason the Cisco Unified Communications Manager cannot open the device or associated lines when it comes back into service, the CTIManager closes the device and lines.

**CTIManager**

When a CTIManager fails, the applications that are connected to the CTIManager can recover the affected resources by reopening these devices on another CTIManager. An application determines which CTIManager to use on the basis of CTIManagers that you defined as primary and backup when you set up the application (if supported by the application). When the application connects to the new CTIManager, it can reopen the devices and lines that previously opened. An application can reopen a Cisco Unified IP Phone before the phone rehomes to the new Cisco Unified Communications Manager; however, it cannot control the phone until the rehoming completes.

---

**Note**
The applications do not rehome to the primary CTIManager when it comes back in service. Applications fail back to the primary CTIManager if you restart the application or if the backup CTIManager fails.

---

**Application failure**

In the Application Heartbeat Maximum Interval and Application Heartbeat Minimum Interval advanced service parameters, you define the interval at which CTIManager expects to receive a message from the application within two consecutive intervals. When an application (TAPI/JTAPI or an application that directly connects to the CTIManager) fails, the CTIManager closes the application and redirects unterminated calls at CTI ports and route points to the configured call forward on failure (CFOF) number. The CTIManager also routes subsequent calls into those CTI ports and route points to the configured Call Forward No Answer (CFNA) number until the application recovers and reregisters those devices.
CTI redundancy
Cisco ATA 186

This chapter provides information about the Cisco ATA 186 Analog Telephone Adaptor functions as an analog telephone adapter that interfaces regular analog telephones to IP-based telephony networks. The Cisco ATA converts any regular analog telephone into an Internet telephone. Each adapter supports two voice ports, each with its own telephone number.

- Configure Cisco ATA, page 587
- Cisco ATA 186 features, page 587
- Connecting with Cisco Unified Communications Manager, page 588

Configure Cisco ATA

The Cisco ATA 186 Analog Telephone Adaptor functions as an analog telephone adapter that interfaces regular analog telephones to IP-based telephony networks. The Cisco ATA converts any regular analog telephone into an Internet telephone. Each adapter supports two voice ports, each with its own telephone number.

To configure the Cisco ATA refer to the following steps.

Procedure

Step 1 Configure the Cisco ATA in Cisco Unified Communications Manager Administration.
Step 2 Install the Cisco ATA.
Step 3 Make a call.

Cisco ATA 186 features

The following list describes the Cisco ATA:

- Contains a single 10 BaseT RJ-45 port and two RJ-11 FXS standard analog telephone ports
- Supports G.711 alaw, G.711 mulaw, and G.723 and G.729a voice codecs
• Uses the Skinny Client Control Protocol
• Converts voice into IP data packets that are sent over a network
• Supports redial, speed dial, call forwarding, call waiting, call hold, transfer, conference, voice messaging, message-waiting indication, off-hook ringing, caller-ID, callee-ID, and call waiting caller-ID

Connecting with Cisco Unified Communications Manager

Like other IP devices, the Cisco ATA receives its configuration file and list of Cisco Unified Communications Managers from the TFTP server. If the TFTP server does not have a configuration file, the Cisco ATA uses the TFTP server name or IP address and port number as the primary Cisco Unified Communications Manager name or IP address and port number.

After the Cisco ATA initializes, both ports on the Cisco ATA (skinny clients) attempt to connect with the primary Cisco Unified Communications Manager. If the connection or registration fails, the Cisco ATA skinny clients attempt to register with the next Cisco Unified Communications Manager in the Cisco Unified Communications Manager list. If that connection fails, the Cisco ATA skinny clients attempt to register with the last Cisco Unified Communications Manager in the list. If all attempts to connect and register with a Cisco Unified Communications Manager fail, the client attempts to connect at a later time.

Upon successful registration, the Cisco ATA client requests the Cisco Unified Communications Manager software version, current time and date, line status, and call forward status from the Cisco Unified Communications Manager. If the Cisco ATA loses connection to the active Cisco Unified Communications Manager, it attempts to connect to a backup Cisco Unified Communications Manager in the Cisco Unified Communications Manager list. When the primary Cisco Unified Communications Manager comes back online, the Cisco ATA attempts to reconnect to it.
Administrative tools overview

This chapter provides information about administrative tools for Cisco Unified Communications Manager administrators.

- Bulk Administration Tool (BAT), page 589
- Cisco Unified Serviceability, page 589
- Call Detail Records, page 590

Bulk Administration Tool (BAT)

The Bulk Administration Tool (BAT), installed with Cisco Unified Communications Manager, lets you add, update, or delete a large number of phones, users, user device profiles, Cisco Unified Communications Manager Assistant managers and assistants, Cisco VG200 gateways and ports, and Cisco Catalyst 6000 24 Port FXS analog interface modules to the Cisco Unified Communications Manager database. Where this was previously a manual operation, BAT helps you automate the process and achieve much faster add, update, and delete operations.

BAT installs as part of the Cisco Unified Communications Manager Administration.

Cisco Unified Serviceability

Administrators can use the Cisco Unified Serviceability web-based tool to troubleshoot problems with the Cisco Unified Communications Manager system. Cisco Unified Serviceability provides the following services:

- Saves Cisco CallManager services alarms and events for troubleshooting and provides alarm message definitions.
- Saves Cisco CallManager services trace information to various log files for troubleshooting. Administrators can configure, collect, and view trace information.
- Monitors real-time behavior of the components in a Cisco Unified Communications Manager system.
- Generates reports for Quality of Service, traffic, and billing information through Cisco CDR Analysis and Reporting (CAR) application.
• Provides feature services that you can activate, deactivate, and view through the Service Activation window.
• Provides an interface for starting and stopping feature and network services.
• Archives reports that are associated with Cisco Unified Serviceability tools.
• Allows Cisco Unified Communications Manager to work as a managed device for SNMP remote management and troubleshooting.
• Monitors the disk usage of the log partition on the server(s).

To access Serviceability from the Cisco Unified Communications Manager Administration window, choose Cisco Unified Serviceability from the Navigation drop-down list box that displays in the upper, right corner of the window and click Go.

CDR Analysis and Reporting (CAR)

CAR, a web-based reporting application, generates reports based on the call detail records (CDRs) and call management records (CMRs) that Cisco Unified Communications Manager collects. CAR processes the CDR and CMR flat files that the CDR Repository service places in the CDR repository and stores the information in the CAR database. CAR uses the information to generate reports that provide information regarding voice quality, traffic, and billing.

To access CAR, administrators must activate the CAR services in Cisco Unified Serviceability. After you activate the appropriate services, administrators can access CAR through a secured login from the Cisco Unified Serviceability Tools menu. End users and managers can access a subset of the reports through a URL that you provide to them.

To view the reports, you must use Adobe Acrobat Reader, which you can download and install from the CAR main window. You can also save reports as CSV files.

Call Detail Records

When CDR collection is enabled through the CDR Enabled Flag Cisco CallManager service parameter, Cisco Unified Communications Manager writes call detail records (CDRs) to flat files on the subsequent servers as calls are completed. When CDR Diagnostic collection is enabled through the Call Diagnostics Enabled Cisco CallManager service parameter, Cisco Unified Communications Manager writes call detail diagnostic records to flat files on the subsequent servers as calls are completed. The CDR Repository Manager service maintains the CDR and CMR files, sends files to preconfigured destinations, and manages the disk usage of the files. CAR accesses the CDR/CMR files in the directory structure that the CDR Repository Manager service creates.

Enable and configure CDR collection through service and enterprise parameters that are set in Cisco Unified Communications Manager Administration. For Standalone edition, enable CDR collection on each Cisco Unified Communications Manager in the cluster for which you want to generate records.

The following service parameters apply to CDRs:

• CDR Enabled Flag-Cisco CallManager service parameter that controls whether CDRs are generated. For Standalone edition, set this parameter on each Cisco Unified Communications Manager in the cluster. You do not need to restart the Cisco Unified Communications Manager for the change to take effect.

• CDR Log Calls With Zero Duration Flag-Cisco CallManager service parameter that controls whether calls with zero duration are logged in CDRs. The default specifies False (zero duration calls not logged).
• Call Diagnostics Enabled-Cisco CallManager service parameter that controls whether call diagnostic records that contain QoS information about calls are generated. The default specifies False (diagnostics not generated).

The following enterprise parameters apply to CDRs:

• CDR File Time Interval-The parameter that determines how many seconds to write to a CDR file before Cisco Unified Communications Manager closes the CDR file and opens a new one.

• Cluster ID-Parameter that provides a unique identifier for the cluster. This parameter gets used in CDR records, so collections of CDR records from multiple clusters can be traced to the sources. The default specifies StandAloneCluster. Cisco does not support clusters for Cisco Unified Communications Manager Business Edition 5000 systems.

Use the CDR Management window in Cisco Unified Serviceability to set the amount of disk space to allocate to CDR and CMR files, configure the number of days to preserve files before deletion, and configure up to three billing application server destinations for CDRs.
INDEX

A

AAR 144
    automated alternate routing (AAR) 144
abbreviated dial 536
    described 536
access log 26
ad hoc conferences 273, 274, 276, 277, 278, 279, 280
    Advanced Ad Hoc Conference Enabled 278
    description 273
    Drop Ad Hoc Conference 277
    initiating 273
    limitations 280
    linear conference linking 274
    Non-linear Ad Hoc Conference Linking Enabled 278
    nonlinear conference linking 274
    party entrance tone 280
    restrictions for phone that is running SIP 279
    service parameters 276
    using cBarge softkey 273
    using Join softkey 273
administrator tools 589, 590
    BAT 589
    CAR 590
    Cisco Unified Serviceability 589
    overview 589
admission control 48, 65
Advanced Ad Hoc Conference Enabled service parameter 278
alarms 131
    DHCP 131
alternate routing 570
    video 570
amwi 520
    described 520
analog telephony protocols 383, 384
    CAS 384
    described 383
    E&M signaling 384
    ground-start signaling 383
    loop-start signaling 383
announcements 263
    announcements (table) 263
annunciator 257, 258, 261, 262, 263, 264
    announcements 263
    announcements (table) 263
    configuration checklist (table) 257
    dependency records 264
    limitations 262
    overview 257
    planning configuration 261
    system requirements 262
    tones 263
    troubleshooting 264
    understanding 258
appliance 3
application dial rules 203, 204
    configuration design 203
    configuration error checking 204
application profiles 236
application user 233, 234, 236
    associating devices 236
    configuration checklist (table) 233
    described 233, 234
ATA 186 features 587
audio quality 65
authentication 229, 240
    user 229
    using with credential policy 240
automated alternate routing (AAR) 144, 146
    and hunt pilots 146
    and remote gateways 146
    described 144
    dial prefix matrix example (table) 144
    enable service parameter 146
    example 144
    line/DN and AAR groups (table) 144
autoregistration 125, 126, 127
    configuration checklist (table) 125
    described 125
    multiple protocol support 127
    understanding 126
B
back to back user agent 438
SIP 438
balanced call processing 56
explained 56
bandwidth 37, 65, 71, 568
allocation of 65
calculations for admission control 71
management for video 568
used by codec types (table) 37
barge 521
described 521
Basic Rate Interface (BRI) 359, 385
BAT 589
BLF buttons 509
BRI 359
Bulk Administration Tool 589
BAT 589
Busy Lamp Field (BLF) buttons 509
buttons 540
directories 540
messages 540

C
call admission control 48, 65, 68, 74, 76, 94
gatekeepers 74, 76
components 76
explained 74
in a distributed setting (figure) 74
locations 68
explained 68
illustrated (figure) 68
overview 65
RSVP and IPv6 94
trunks 74
call diversion (forwarding), QSIG supplementary service 389
call failure, avoiding 299
call forward 198, 321, 413, 521
call forward all 521
call forward all loop prevention 521
CFA destination override 521
described 521
call forward busy 521
described 521
call forward no answer 521
described 521
call forward no coverage 521
described 521
described 198
in multiple voice-mail systems 321
multiple voice-mail systems examples 321
SIP 413
call forward busy 521
described 521
call forward no answer 521
described 521
call forward no coverage 521
described 521
call forwarding 153
described 153
call hold 413
SIP 413
call park 525
described 525
call park Busy Lamp Field (BLF) buttons 509
call pickup 343, 525
described 343, 525
call preservation 121, 122
explained 121
scenarios (table) 122
call processing 7, 56, 61
balanced load explained 56
by Cisco Unified Communications Manager 7
combined with redundancy (figure) 61
call select 526
described 526
call transfer 322, 390, 413
QSIG supplementary service 390
SIP 413
using hookflash 322
call waiting 198
described 198
called party 151, 177, 181
transformations 151, 177
transformations settings 181
transformations settings (table) 181
caller identification 184, 188
restrictions 184
support for device control protocols (table) 188
caller identification (continued)
  support vs. device control protocols 188
types 184
calling line 414
  SIP 414
calling name presentation 414
  SIP 414
calling party 160, 177, 178, 184
  normalization 160
  presentation settings 184
  restriction settings 184
  transformations 177
  transformations settings 178
  transformations settings (table) 178, 184
calling search spaces 135, 137, 538
  dependency records 137
  examples 135
  explained 135
  guidelines and tips 137
  list of topics 135
  search for phones 538
calls 199, 532, 545
  making and receiving multiple per directory number 199
  on-hook call transfer 532
  video 545
CAR overview 590
Catalyst 4000 364
  4224 voice gateway switch 364
  access gateway module 364
Catalyst 4224 Voice Gateway Switch 364
Catalyst 6000 308, 363, 364
  Cisco Communication Media Module 364
  configuration illustrated (figure) 308
  FXS analog interface module 363
  hookflash transfer 363
  T1/E1 line card 363
CDR 590
  described 590
CDR Analysis and Reporting (CAR) 590
centralized TFTP 116, 117
  configuration tips 117
  master TFTP server 116
  overview 116
  secure clusters 116
CFA Destination Override service parameter 198, 521
channel associated signaling (CAS) 359, 384
characters, special 161, 166
  configuring 161
  described (table) 166
Cisco ATA 186 587, 588
  configuration checklist (table) 587
  connecting to Cisco Unified Communications Manager 588
Cisco Call Back 389
  described 389
Cisco Catalyst 4000 307
Cisco Catalyst 6000 308
Cisco Communication Media Module (CMM) 364
Cisco Conference Bridge (WS-SVC-CMM) 268
Cisco DPA 335, 336
  illustrated (figure) 336
  integration overview 335
Cisco DSP 303, 307, 309, 310
  NM-HD supported gateways 310
  NM-HDV supported gateways 309
  NM-HDV2 supported gateways 310
  overview 303
  supported gateways 307
  supported routers 307
  understanding 303
Cisco IP Communicator 500, 504
  default phone button template 504
  described 500
Cisco IP SoftPhone profiles 238
Cisco Messaging Interface 327
  CMI 327
Cisco SIP endpoints 444
  SIP profile 444
Cisco TelePresence 501
  described 501
Cisco TFTP service 105, 106, 110, 115
  alternate Cisco file servers 115
  configuration checklist (table) 106
  list of topics 105
  overview 105
  understanding 110
Cisco Unified CM User Options 541
Cisco Unified Communications 5, 6, 7, 8, 11
  applications 6
  call processing 7
  client 7
  clients 7
  components 6
  configuring system 11
  infrastructure 7
  network 8
  overview 5
  support 6
  supported applications 6
Cisco Unified Communications Manager 3, 4, 7, 30, 33, 37, 59, 291, 300, 315, 584
  bandwidth usage 37
  becoming inactive 291, 300
  benefits 4
  call processing 7
  configuration 33
  CTI redundancy 584
  groups 33, 59
  configuring 33

Cisco Unified Communications Manager System Guide, Release 9.0(1)
Cisco Unified Communications Manager *(continued)*

- groups *(continued)*
  - described 59
  - illustrated (figure) 59
- introduction 3
- key features 4
- redundancy 59
- server, configuring 30
- supported voice codecs 37
- voice mail connectivity 315

Cisco Unified Communications Manager Assistant 514
- softkey templates 514
  - described 514

Cisco Unified Communications Manager JTAPI 241
- using credential policy 241
- using user directory 241

Cisco Unified Communications Manager TAPI 241
- using credential policy 241

Cisco Unified IP Phone Services 345, 347, 349
- configuration checklist (table) 345
- dependency records 349
- guidelines and tips 349
- overview 345
- understanding 347

Cisco Unified IP Phones 35, 113, 443, 459, 462, 504, 520, 521, 525, 526, 527, 528, 530, 531, 532, 534, 535, 536, 537, 540
- 12 SP+, described 462
- 30 VIP, described 462
- 3951 462
- 7902, described 462
- 7905, described 462
- 7906, described 462
- 7910, described 462
- 7911, described 462
- 7912, described 462
- 7914 Expansion Module, described 462
- 7940, described 462
- 7941, described 462
- 7960, described 462
- 7961, described 462
- 7970, described 462
- 7971, described 462
- 7985, described 462
- Cisco Unified IP Conference Station 7935, described 462
- Cisco Unified IP Conference Station 7936, described 462
- directories button 540
- features 520, 521, 525, 526, 527, 528, 530, 531, 532, 534, 535, 536, 537
  - abbreviated dial 536
  - audible message waiting indicator 520
  - barge 521
  - call diagnostics and voice quality metrics 525
  - call forward all 521
  - call forward busy 521
  - call forward no answer 521
  - call forward no coverage 521
  - call park 525
  - call pickup 525, 526
  - call select 526
  - conference linking 526
  - conference list 527
  - connected number display 527
  - described 520
  - device mobility 527
  - direct transfer 527
  - directed call park 527
  - do not disturb 528
  - hold reversion 530
  - immediate divert 530
  - intercom 531
  - IPv6 531
  - join 531
  - log out of hunt groups 531
  - malicious call ID 532
  - mobile connect and mobile voice access 532
  - monitoring and recording 532
  - peer-to-peer image distribution 534
  - privacy 521
  - quality report tool 535
  - secure tone 536
  - service URL 536
  - speed dial 536
  - VPN client 537
  - identifying TFTP server 113
  - messages button 540
  - overview 459
- SIP 462
  - 3951, described 462
  - supported models 462
  - that are running SIP 35, 462, 504
  - default phone button template (advanced) 462, 504
  - default phone button template (basic) 462, 504
  - NTP reference 35
  - that support SIP 443
- PLAR 443
  - Cisco Unified Mobile Communicator 501
  - described 501
- Cisco Unified Personal Communicator 500
  - described 500
- Cisco Unity 331, 332, 333
  - configuration checklist (table) 331
  - connections with the phone system (figure) 333
  - messaging integration 331, 333
  - description 333
  - overview 331
  - system requirements 332
Cisco VG200 Voice Gateway 361
Cisco VG224 Analog Phone Gateway 361
configuring 361
description 361
Cisco VG248 Analog Phone Gateway 360, 378
configuring 360
description 360
gateway redundancy 378
Cisco Wireless IP Phones 462
7920, described 462
clear filter button 538
phone search 538
closest match routing 156
clusters 53, 54, 55, 56, 59
balanced call processing 56
communication between 55
compared to groups 59
configuration checklist (table) 53
database replication 54
described 54
list of topics 53
overview 53
CMI redundancy 327
described 327
illustrated (figure) 327
CMLocal date/time group 35
codes 37, 546
bandwidth used per call (table) 37
G.711 37
G.723 37
G.729 37
GSM 37
video 546
wideband 37
common device configurations 47, 538
described 47
search for phones 538
common phone profiles 518
described 518
communication between clusters 55
compression of voice stream 305
Computer Telephony Integration 577
CTI 577
conference bridges 265, 268, 273, 284, 285
ad hoc 273
described 273
annunciator 268
configuration checklist (table) 265
dependency records 284
meet-me 273
described 273
overview 265
performance monitoring 285
troubleshooting 285
conference bridges (continued)
types (table) 268
types in Cisco Unified Communications Manager Administration 268
conference chaining 280
conference devices 266, 267, 268
Cisco Conference Bridge (WS-SVC-CMM), described 268
MTP WS-X6608 DSP service card 268
software, described 267
understanding 266
video, described 267
conference linking 526
described 526
conference list 527
described 527
conference routers 266
described 266
conferences 200, 273, 280
ad hoc 273, 280
initiating 273
limitations 280
described 200
meet-me 280
initiating 280
limitations 280
party entrance tone 280
conferencing 303, 305, 306, 571
across an IP WAN 305
hardware-based 306
using Cisco DSP 303
video 571
configuration 29, 33, 120
Cisco Unified Communications Manager 33
files for devices 120
settings 29
checklist (table) 29
list of topics 29
configuration checklist 358
MGCP BRI 358
connected line, SIP 416
connected name identification, SIP 416
connected number display 527
described 527
connected party 186
presentation settings 186
restriction settings 186
transformations settings (table) 186
counters, video bridge 575
credential management 236
credential policy 239, 240, 241, 242
bulk administration 241
configuration checklist (table) 240
credential caching 241
credential history 241
credential policy (continued)
described 239
events 242
JTAPI/TAPI support 241
logs 242
using with authentication 240
CTI 63, 445, 479, 577, 578, 579, 580, 582, 583, 584, 585
application failure 585
applications 578
configuration checklist (table) 577
controlled devices 580
CTIManager 579, 585
described 579
redundancy 585
dependency records 584
IP phones 580
IPv6 support 584
list of topics 577
media termination points 580
ports 479, 580
described 479, 580
redundancy 63, 584
route points 580
SIP endpoints 445
super provider 583
user groups 582
user management 582

dependency records (continued)
partitions 137
phones 541
described 541
system-level settings 51
time periods 141
time schedules 141
transcoders 292
device control protocols and caller identification support
table 188
device mobility 527
described 527
device pools 45, 47, 121, 538
described 45, 121
search for phones 538
updating 47
devices 61, 110, 112, 113, 119, 120, 121, 236, 237, 266, 267, 268, 291, 299, 580
accessing TFTP server 112
associating to an application user 236
associating to an end user 237
associating with users 236
conference 266, 267, 268
Cisco Conference Bridge (WS-SVC-CMM) 268
software 267
understanding 266
video 267
configuration files 120
CTI control 580
distributing for redundancy 61
firmware loads 120
identifying TFTP server 113
MTP characteristics 299
support 119
list of topics 119
supported 119
transcoders 291
resetting 291
updating firmware loads 121
using Cisco TFTP 110
using DHCP 110
DHCP 110, 129, 130, 131
alarms 131
and devices 110
domain name system 130
migration 131
server 129, 131
configuration process 131
described 129
TFTP 131
dial plans 374
accessing gateways 374
dial rules 203
overview 203
digit analysis, static 158
caveats 158
configuration tip 158
described 158
explained 158
Unified Communications Manager Assistant example 158
digital signal processor (DSP) 303
digital telephony protocols 385, 386
BRI 385
described 385
E1 PRI 386
QSIG 386
T1 PRI 385
direct transfer 200, 527
described 200, 527
directed call park 527
described 527
directories button, configuring 540
directory 48, 225, 226, 228, 230, 233, 238
access 228
access for Cisco Unified Communications endpoints 230
configuration checklist (table) 226, 233
extension mobility 238
LDAP 48
overview 225
directory lookup dial rules overview 205
directory numbers 191, 192, 193, 197, 198, 199, 200, 201, 202, 521
active check box 197
call forward 198, 521
busy trigger 198, 521
no answer ring duration 198, 521
call forward information display 198, 521
characteristics 192
conference 200
configuration checklist (table) 191
dependency records 202
described 202
direct transfer 200
features 198
call forward 198
call waiting 198
listed 198
find all directory numbers 201
join 200
making and receiving multiple calls 199
managing 197
overview 191
search tips 201
shared line appearance 193
shared line appearance restrictions 193
transfer 200
update directory number of all devices sharing this line check box 197
discard digits instructions 157, 169
configuring 169
explained (table) 169
DND 528
described 528
DNs 191
directory numbers 191
DPA 7630/7610 335, 336, 337
functionality 336
illustrated (figure) 336
purpose 336
understanding 335
using SMDI 336, 337
Drop Ad Hoc Conference service parameter 277
DSCP 444, 570
marking 570
SIP 444
DTMF digits 411
SIP devices 411

e
E&M signaling 384
delay dial 384
immediate start 384
wink start 384
E1 CAS 385
E1 Primary Rate Interface (E1 PRI) 386
E1 Primary Rate Interface (PRI) 359
Effective Access Privileges For Overlapping User Groups and Roles enterprise parameter 26
drop user 233, 235, 237
associating devices 237
customization checklist (table) 233
described 233, 235
enterprise parameters 26, 51
described 51
Effective Access Privileges For Overlapping User Groups and Roles 26
user groups 26
expansion module 462
Cisco Unified IP Phone 7914 462
extension mobility 238, 351
described 351
user device profile 238
user directory 238
external calls 154
forwarding 154
features 293, 341, 345, 351, 353, 509
   call park 341
   Cisco Unified Communications Manager Assistant 353
   Cisco Unified IP Phone Services 345
directed call park 341
   extension mobility overview 351
   music on hold (MOH) 293
   phone button features (table) 509
   phone login overview 351
fields requiring route patterns (table) 166
firewall 249
   traversal 249
firmware loads 120, 121
   described 120
   updating 121
Foreign Exchange Office (FXO) 359, 383
Foreign Exchange Station (FXS) 359, 383
forwarding 154
   internal and external calls 154
FXO 359, 383
FXS 359, 383
g.711 37
G.723 37
G.729 37
g.clear codec 418
   SIP trunks 418
gatekeepers 67, 74, 76, 77, 451, 549
   and call admission control (figure) 74
   configuration checklist (table) 67
   configuring 76
   configuring in Cisco Unified Communications Manager 77, 451
   configuring on the router 76
   described 74
   H.323 549
gateways 113, 308, 357, 359, 360, 361, 363, 364, 365, 374, 375, 376, 571
   Catalyst 4000 Access Gateway Module 364
   Catalyst 4224 gateway 364
   Catalyst 6000 configuration illustrated (figure) 308
   Catalyst 6000 FXS Analog Interface Module 363
   Catalyst 6000 T1/E1 and Services Module 363
   Cisco Communication Media Module 364
   Cisco IOS H.323 devices 365
   Cisco voice gateways 359
   configuration checklist (table) 357
   dependency records 375
   failover and fallback 376
   H.323 devices 365
gateways (continued)
   identifying TFTP server 113
   models (table) 365
   overview 357
   port types (table) 365
   related to dial plans 374
   signaling protocols (table) 365
   standalone 360, 361
      VG200 voice 361
      VG224 analog phone 361
      VG248 analog phone 360
   summary of voice gateways (table) 365
   timer parameter for video 571
   trunk interfaces (table) 365
   ground-start signaling 383
groups, Cisco Unified Communications Manager 33, 59
   compared to clusters 59
   components of 59
   configuring 33
   illustrated (figure) 59
   groups, date/time 35
   GSM 37

H
H.323 365, 377, 381, 479, 549, 550, 571
call processing 550
   Cisco IOS gateways 365
   clients 479
   configuration notes 550
dynamic addressing 549
gateways 365
   IOS gateway redundancy 377
   registering with gatekeeper 549
   trunk interaction for video 571
   used in voice gateways 381
   video 549
   hold 193
   viewing held calls on shared lines 193
   hold reversion 530
   described 530
   hookflash transfer 363
   hub-and-spoke topology 65
   hunt lists 152, 154, 155, 156
   described 152
      hunt group logoff notification service parameter 156
      log out of hunt groups 154
      log out of hunt groups softkey 155
      non-shared-line operation 156
      shared-line operation 156
   hunt pilots 146, 152, 166
      and automated alternate routing 146
hunt pilots (continued)
  described 152
  wildcards 166
hunting 153, 154
  described 153
  example 153
  maximum hunt timer 154
  personal preferences 154

I
identification services 392
  QSIG supplementary service, described 392
immediate divert 530
  described 530
Intelligent Bridge Selection 281
inter-VRF communication 249
intercluster communication 55
intercluster voice mail 315
intercom 531
  described 531
internal calls 154
  forwarding 154
international escape character + 161
  benefits 161
  configuring \+ 161
  configuring + 161
  gateway and trunk support 161
  phone support 161
  speed dial support 161
  SRST support 161
  String + on Outbound Calls service parameter 161
internet ecosystem 5
introduction to Cisco Unified Communications Manager 3
IP Phone Services 345
  Cisco Unified IP Phone Services 345
IP Phones 459
  Cisco Unified IP Phones 459
IP telephony protocols 381
  understanding 381

J
join 200, 531
  described 200, 531
  party entrance tone 200
JTAPI 241
  Cisco Unified Communications Manager JTAPI 241

L
LDAP 48, 225
  described 48
  overview 225
line groups 152
  described 152
linear ad hoc conference linking 274
load balancing 56, 61
  distributing devices 61
  explained 56
load, firmware 120
local route groups 151
locations 37, 65, 66, 68, 70, 80
  and call admission control (figure) 68
  and regions 37
  configuration checklist (table) 66, 80
  described 68
  interaction with regions 70
  interaction with regions (figure) 70
  used in admission control 65
log out of hunt groups 154, 155, 531
  described 154, 155, 531
  softkey 155
logging missed calls for shared lines 193
loop-start signaling 383

M
malicious call ID 532
  described 532
master TFTP server 116
  sending files to the master TFTP server 116
maximum hunt timer 154
media 249
  firewall traversal 249
  media control 246
Media Gateway Control Protocol (MGCP) 382
  media resource group lists 245, 253, 255
  configuration checklist (table) 245
  dependency records 255
  described 253
  media resource groups 245, 252, 255
  configuration checklist (table) 245
  dependency records 255
  described 252
  media resource manager 288, 297
  managing MTPs 297
  using to manage transcoders 288
media resources 62, 245, 246, 252, 253
  call control 246
  described 246
  management 245
media resources (continued)
  media control 246
  media resource group lists 253
  media resource groups 252
  media termination point control 246
  music on hold control 246
  overview 245
  redundancy 62
  unicast bridge control 246
media termination points 295
MTP 295
meet-me conferences 273, 280
  description 273
  initiating 280
  limitations 280
  party entrance tone 280
message waiting 318
  description 318
  indication 318
messages button 540
messaging, Cisco Unity 331, 333
  integration description 333
  integration overview 331
MGCP 358, 362, 377, 382
  BRI 358, 362
    call flow (figure) 362
    configuring 358
    described 382
    gateway redundancy 377
migrating phones 519
missed calls 193
  logging missed calls for shared lines 193
MLPP 50, 420
  described 50
  Resource Priority Namespace Network Domains 420
  SIP trunks and VoSIP 420
mobile connect and mobile voice access 532
  described 532
modifying files 117
MOH 246, 293
  described 293
  MOH control 246
monitoring and recording 532
  described 532
MTP 246, 268, 288, 295, 296, 297, 298, 299, 300, 301, 304, 399, 400, 412, 580
  avoiding call failure/user alert 299
  Cisco Unified Communications Manager becomes inactive 300
  configuration checklist (table) 295
  control 246
  CTI 580
  dependency records 301
  device characteristics 299
MTP (continued)
  failover and fallback 300
  managing with media resource manager 297
  overview 295
  planning configuration 298
  resetting registered devices 300
  SIP 399
  SIP devices 400
  supplementary services for a SIP call 412
  system requirements and limitations 300
  transcoding services 304
  types (table) 298
  understanding 296
  using transcoders 288
  WS-X6608 DSP service card 268
multisite WAN 305
  using centralized MTP transcoding (figure) 305
music on hold 293
  MOH 293

N

network 249
  virtualization 249
    inter-VRF communication 249
    media firewall traversal 249
network video 547
NM-HD supported gateways 310
NM-HDV supported gateways 309
NM-HDV2 supported gateways 310
Non-linear Ad Hoc Conference Linking Enabled service parameter 278
nonlinear ad hoc conference linking 274
normalization 160, 407
  calling party 160
  description 407
NTP SIP 444

O

on-hook call transfer 532
overview 3, 11
  of Cisco Unified Communications Manager 3
  of system configuration 11

P

parameters 26, 51, 318, 541
  enterprise 26, 51
  described 51
parameters (continued)
enterprise (continued)
  Effective Access Privileges For Overlapping User
  Groups and Roles  26
  user groups  26
service  51, 318, 541
  described  51
  Maximum Phone FallBack Queue Depth  541
  Message Waiting Lamp Policy  318
partitions  135, 137
  dependency records  137
  examples  135
  explained  135
  guidelines and tips  137
  list of topics  135
  name limitations  137
party entrance tone  200, 280
  conferences  280
  join  200
path replacement  394
  described  394
peer-to-peer image distribution  534
  described  534
performance monitoring counters  574
  video  574
personal preferences  154
phone button templates  462, 504, 512
  12 series, default template  504
  30 SP+, default template  504
  30 VIP, default template  504
  7902, default template  504
  7905 SCCP, default template  504
  7905 SIP, default template  504
  7906 SCCP, default template  504
  7906 SIP, default template  504
  7910, default template  504
  7911 SCCP, default template  504
  7911 SIP, default template  504
  7912 SCCP, default template  504
  7912 SIP, default template  504
  7920, default template  504
  7931, default template  504
  7940 SCCP, default template  504
  7940 SIP, default template  504
  7941 G-GE SCCP, default template  504
  7941 SCCP, default template  504
  7941 SIP, default template  504
  7960 SCCP, default template  504
  7960 SIP, default template  504
  7961 G-GE SCCP, default template  504
  7961 SCCP, default template  504
  7961 SIP, default template  504
  7970 SCCP, default template  504
  7970 SIP, default template  504
phone button templates (continued)
  7971 SCCP, default template  504
  7971 SIP, default template  504
  7985, default template  504
  analog phone, default template  504
  ATA 186, default template  504
  Cisco IP Communicator, default template  504
  Cisco TelePresence, default template  462, 504
  conference station 7935, default template  504
  conference station 7936, default template  504
  IP-STE, default template  504
  ISDN BRI Phone, default template  504
  programmable line keys  512
  third-party SIP device, default template  462, 504
  Unified Communicator SIP, default template  504
  VGC phone, default template  504
  VGC Virtual, default template  504
phone login  351
  described  351
phone NTP reference  35
  configuring for phones that are running SIP  35
phones  345, 460, 503, 504, 509, 514, 515, 516, 518, 519, 520, 521, 531, 533, 538, 541, 542, 587
  administration tips  538
  associating with users  538
  ATA 186  587
  button templates  503, 504, 509
    default  504
    described  503
    guidelines  509
    listed by model (table)  504
  Cisco Unified IP Phone Services  345
  common phone profiles  518
  dependency records  541
    described  541
  failover and fallback  542
  features  509, 520, 521
    Cisco Unified IP  520
    described (table)  509
    privacy  521
  find all phones  538
  IPv6 support  531
  methods for adding  518
  migrating  519
  prime line support for answering calls  533
  SCCP configuration checklist (table)  460
  search by authentication string  538
  search by call pickup group  538
  search by calling search space  538
  search by common device configuration  538
  search by description  538
  search by device name  538
  search by device pool  538
  search by device protocol  538
phones (continued)
search by device type 538
search by directory number 538
search by LSC status 538
search by security profile 538
search criteria 538
search tips 538
SIP configuration checklist (table) 460
softkey templates 514, 515, 516
add application 515
configure softkey layout 516
described 514
PLAR 209, 443
for Cisco phones that support SIP 443
for Cisco Unified IP Phones that support SIP 443
SIP dial rules 209
ports 327, 479
configuring for SMDI 327
CTI 479
described 479
presentation settings 184, 186
calling party 184
connected party 186
preservation of calls 121, 122
explained 121
scenarios (table) 122
prime line 319, 533
support for answering calls 533
support for voice messaging 319
privacy 521
described 521
private line automatic ringdown 209
PLAR 209
profiles 238, 518
Cisco IP SoftPhone 238
common phone 518
programmable line keys 512
overview 512
protocols 315, 360, 374, 377, 381, 382, 383
analog telephony 383
H.323 315, 381
MGCP 382
Session Initiation Protocol (SIP) 382
Skinny Client Control Protocol 360, 382
Skinny Client Control Protocol (SCCP) Gateway Protocol 377
Skinny Gateway Protocol 374
Q
Q signaling 386
QSIG 386
QoS enforcement 250

QSIG 386, 387, 389, 390, 391, 392, 393, 394, 395, 422
Annex M.1 387
basic call feature 389
basic call setup 389
call completion 389
call diversion (rerouting) 389
call transfer 390
Cisco Unified Communications Manager interface 395
compatibility with older versions (ECMA) 391
facility selection and reservation 391
identification services 392
message tunneling 387
message waiting indication (MWI) service 393
overview 386
path replacement 394
SIP trunk 387
supplementary services 389, 390, 392, 394

call completion (Cisco Call Back), described 389
call diversion (forwarding) 389
call transfer 390
identification 392
path replacement 394
tunneling over SIP trunks 422
quality of sound 65
quality report tool 535
described 535
R
redirecting dial number identification service 417
redundancy 59, 61, 62, 63, 327, 376, 377, 378, 584, 585
and distributed call processing (figure) 61
Cisco VG248 378
CMI 327
described 327
illustrated (figure) 327
CTI 63, 584
CTI and Cisco Unified Communications Manager 584
CTIManager 585
IOS H.323 gateways 377
list of topics 59
MGCP gateway 377
of media resources 62
support for gateways 376
types of 59
with distributed call processing 61
regions 37, 70, 400
and call admission control 37
and locations 37
described 37
example (figure) 37
interaction with locations 70
regions (continued)

interaction with locations (figure) 70
SIP devices with MTP 400
used with admission control 70
used with admission control (figure) 70
requirements 332
Cisco Unity 332
restriction settings 184, 186
calling party 184
connected party 186
RFC4028 session timers 443
roles 15, 16, 26
described 15, 16
enterprise parameters 26
overview 15
route groups 147, 151, 374
described 147
local 151
and called party transformations 151
related to dial plans 374
route lists 147
described 147
types, example (figure) 147
route patterns 148, 149, 156, 157, 158
closest match routing 156
considerations for using 148
described 148
fields in Cisco Unified Communications Manager (table) 166
usage 149
using the @ wildcard character 157
wildcards 166
route plans 143, 146, 149, 189
and Cisco Analog Access Gateways (figure) 149
and Cisco Digital Access Gateways (figure) 149
overview 146
report 189
understanding 143
routers, conference 266
hardware 266
routing 139, 140, 141, 144, 154, 156
automated alternate 144
described 144
closest match 156
log out of hunt groups 154
time-of-day 139, 140, 141
dependency records 141
for end users 141
time periods 139
time schedules 140
understanding 139
RSVP 80, 83, 85, 93, 94, 95, 96, 97, 98, 100, 101, 102, 569
call detail records 100
call transfer (example) 97
caveats 83
RSVP (continued)
configuration checklist (table) 80
configuring 85
IPv6 support 94
migrating to 93
MLPP support (examples) 98
music on hold interaction (example) 96
overview 80
shared-line support (example) 95
troubleshooting 100, 101, 102
alarms 101
described
end-to-end RSVP 102
performance monitoring counters 100
trace 101
video support 569
S
SCCP auto-registration 127
search 201, 538
by authentication string 538
by call pickup group 538
by calling search space 538
by common device configuration 538
by description 538
by device name 538
by device pool 538
by device protocol 538
by device type 538
by directory number 201, 538
by LSC status 538
by security profile 538
for all directory numbers in the database 201
for all phones in the database 538
for directory numbers 201
for phones 538
search criteria 538
secure tone 536
described 536
security profiles 404, 538
search for phones 538
SIP trunk 404
server, Cisco Unified Communications Manager 30
configuring 30
service parameters 51, 146, 154, 156, 198, 250, 277, 278, 318, 457, 521, 541
Advanced Ad Hoc Conference Enabled 278
Automated Alternate Routing Enable 146
blocking transfer capabilities 457
call classification 457
CFA Destination Override 198, 521
described 51
Cisco Unified Communications Manager System Guide, Release 9.0(1)
service parameters (continued)
  Drop Ad Hoc Conference 277
  hunt group logoff notification 156
  Maximum Phone FallBack Queue Depth 541
  Message Waiting Lamp Policy 318
  Non-linear Ad Hoc Conference Linking Enabled 278
  Show Line Group Member DN in final Called Party Number
  CDR Field 154
  trusted relay point 250
service URL 536
  described 536
Serviceability 574
  and video 574
Session Initiation Protocol (SIP) 397
  understanding 397
settings 29, 161, 178, 181, 184, 186
  called party transformations 181
    configuring 181
    explained (table) 181
  calling party transformations 178, 184
    explained (table) 178, 184
  configuring 29
    checklist (table) 29
    described 29
  connected party transformations 186
    explained (table) 186
  special characters 161
shared line appearance 193, 197
  active check box 197
  described 193
  logging missed calls to shared line 193
  restrictions 193
  update directory number of all devices sharing this line check box 197
  viewing held calls on shared line 193
shared lines 156
  with hunt lists 156
signaling protocols, gateway 365
Simplified Message Desk Interface 325
  SMDI 325
Simplified Message Desk Interface (SMDI) 315
SIP 279, 382, 397, 398, 399, 400, 410, 411, 412, 413, 414, 416, 417, 422, 423, 438, 440, 441, 442, 443, 444, 445, 556
  3PCC 440
ad hoc conference settings 279
B2BUA 438
basic calls between SIP endpoints and Cisco Unified Communications Manager 410
  call forward 413
  call hold 413
  call identification services 413
  call transfer 413
  calling line and name identification presentation 414
SIP (continued)
  Cisco Unified Communications Manager functionality supported by phones that are running SIP 443
  Cisco Unified Communications Manager support for Cisco SIP endpoints 440
  configuring trunk for video calls 556
  connected line and name identification presentation 416
  description of Cisco Unified Communications Manager and SIP 398
dial plans 443
diversion header 441
DSCP 444
DTMF Relay calls between SIP endpoints and Cisco Unified Communications Manager 411
endpoints 413, 445
  CTI support 445
  supplementary services 413
  forwarding DTMF digits 411
functions and features in Cisco Unified Communications Manager 410
  join header 441
  network time protocol 444
  networking 398
  protocol 382
  PUBLISH 423
    configuration tips 423
    service parameters 423
  REFER 440
  remote party ID (RPID) header 441
  remotecc 442
  replaces and referred-by headers 440
  replaces header 441
  RFC3261 440
  RFC3262 440
  RFC3264 440
  RFC3265 + dialog package 442
  RFC3265 + KPML package 442
  RFC3265 + presence package 442
  RFC3265 + RFC3842 MWI package 442
  RFC3311 440
  RFC3514 440
  RFC4028 session timers 443
  RNDIS 417
  service parameters 400
  SIP PUBLISH 422
  softkey handling 443
  supplementary services 412
timers and counters 400
  trunk configuration checklist (table) 397
  understanding 397
  using MTP devices 399
  video 556
  SIP autoregistration 127
SIP dial rules 206, 207, 209
   dial rule parameters 207
dial rule patterns 206
   overview 206
PLAR 209
SIP endpoints 438
   overview 438
SIP profile 404, 444
   Cisco SIP endpoints 444
   SIP trunks 404
SIP standards 440
   Cisco endpoints 440
SIP trunks 404, 405, 407, 421, 422, 423
   between Cisco Unified Communications Manager 4.X and 6.X systems 405
MLPP for VoSIP 420
   PUBLISH 423
   configuration tips 423
QSIG tunneling over SIP support 422
security profiles 404
SIP profile 404
SIP PUBLISH 422
   support for secured V.150.1 MoIP 421
   transparency and normalization 407
Skinny Client Control Protocol 360, 382, 555
   described 382
   used by Cisco VG248 360
video 555
   video bridging 555
Skinny Client Control Protocol (SCCP) Gateway Protocol 377
Skinny Gateway Protocol 374
SMDI 315, 325, 326, 327, 336, 337
   configuration checklist (table) 325
   integration requirements 326
   migration with DPA 7630/7610 336, 337
   port configuration 327
   PSTN gateway interfaces 315
   voice mail integration 315, 325
softkey templates 516, 517
   call states described (table) 516
   layout (figure) 516
   operation 517
softkeys 155, 443
   log out of hunt groups 155
   SIP 443
softphone 500
SoftPhone 238
   Cisco IP SoftPhone 238
sound quality 65
special characters 161, 166
   configuring 161
   described (table) 166
   explained 166
   international escape character + 161
   speed dial 536
      described 536
standards, SIP 440
static digit analysis 158
   caveats 158
   configuration tip 158
   described 158
   explained 158
   Unified Communications Manager Assistant example with static digit analysis 158
supplementary services 413
   initiated by SIP endpoint 413
supported devices 119
switch-based gateways 363
system configuration 11
   for complete IP telephony system 11
      overview 11
system-level configuration settings 29

T

T1 CAS 385
T1 Primary Rate Interface (PRI) 359
T1 Primary Rate Interface (T1 PRI) 385
telephony, video 544
templates, phone button 462, 503, 504, 509
   12 series, default 504
   30 SP+, default 504
   30 VIP, default 504
   7902, default 504
   7905 SCCP, default 504
   7905 SIP, default 504
   7906 SCCP, default 504
   7906 SIP, default 504
   7910, default 504
   7911 SCCP, default 504
   7911 SIP, default 504
   7912 SCCP, default 504
   7912 SIP, default 504
   7920, default 504
   7931, default 504
   7940 SCCP, default 504
   7940 SIP, default 504
   7941 G-GE SCCP, default 504
   7941 SCCP, default 504
   7941 SIP, default 504
   7960 SCCP, default 504
   7960 SIP, default 504
   7961 G-GE SCCP, default 504
   7961 SCCP, default 504
   7961 SIP, default 504
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trivial File Transfer Protocol (TFTP)</td>
<td>105</td>
</tr>
<tr>
<td>TRP</td>
<td>248</td>
</tr>
<tr>
<td>trusted relay point</td>
<td>248</td>
</tr>
<tr>
<td>trunk interfaces</td>
<td></td>
</tr>
<tr>
<td>BRI</td>
<td>359, 385</td>
</tr>
<tr>
<td>E1 CAS</td>
<td>385</td>
</tr>
<tr>
<td>E1 PRI</td>
<td>359, 386</td>
</tr>
<tr>
<td>FXO</td>
<td>359, 383</td>
</tr>
<tr>
<td>FXS</td>
<td>359, 383</td>
</tr>
<tr>
<td>QSIG</td>
<td>386</td>
</tr>
<tr>
<td>signaling</td>
<td></td>
</tr>
<tr>
<td>E&amp;M</td>
<td>384</td>
</tr>
<tr>
<td>ground start</td>
<td>383</td>
</tr>
<tr>
<td>loop start</td>
<td>383</td>
</tr>
<tr>
<td>T1 CAS</td>
<td>359, 385</td>
</tr>
<tr>
<td>T1 PRI</td>
<td>359, 385</td>
</tr>
<tr>
<td>trunks</td>
<td></td>
</tr>
<tr>
<td>67, 74, 76, 77, 397, 404, 449, 451, 452, 453, 456, 457, 458</td>
<td></td>
</tr>
<tr>
<td>associated route groups</td>
<td>458</td>
</tr>
<tr>
<td>call classification settings</td>
<td>456</td>
</tr>
<tr>
<td>configuration</td>
<td>451</td>
</tr>
<tr>
<td>configuration checklist (table)</td>
<td>67, 449</td>
</tr>
<tr>
<td>configuring in Cisco Unified Communications Manager</td>
<td>77, 451</td>
</tr>
<tr>
<td>configuring on the router</td>
<td>76</td>
</tr>
<tr>
<td>configuring transfer</td>
<td>456</td>
</tr>
<tr>
<td>configuring transfer using call classification service parameter</td>
<td>457</td>
</tr>
<tr>
<td>dependency records</td>
<td>458</td>
</tr>
<tr>
<td>described</td>
<td>74</td>
</tr>
<tr>
<td>gatekeeper controlled</td>
<td>451</td>
</tr>
<tr>
<td>non-gatekeeper controlled</td>
<td>452</td>
</tr>
<tr>
<td>overview</td>
<td>449</td>
</tr>
<tr>
<td>SIP configuration checklist</td>
<td>397</td>
</tr>
<tr>
<td>SIP, security profiles</td>
<td>404</td>
</tr>
<tr>
<td>transferring calls</td>
<td>456</td>
</tr>
<tr>
<td>types</td>
<td>452, 453</td>
</tr>
<tr>
<td>H.225 gatekeeper controlled</td>
<td>452</td>
</tr>
<tr>
<td>intercluster gatekeeper controlled</td>
<td>453</td>
</tr>
<tr>
<td>intercluster non-gatekeeper controlled</td>
<td>453</td>
</tr>
<tr>
<td>overview</td>
<td>452</td>
</tr>
<tr>
<td>SIP</td>
<td>453</td>
</tr>
<tr>
<td>trusted relay point</td>
<td>248, 250, 251</td>
</tr>
<tr>
<td>explained</td>
<td>248</td>
</tr>
<tr>
<td>insertion</td>
<td>251</td>
</tr>
<tr>
<td>service parameter</td>
<td>250</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>user</td>
<td>233, 234, 235, 236, 237, 238, 541</td>
</tr>
<tr>
<td>application</td>
<td>233, 234, 236</td>
</tr>
<tr>
<td>associating devices</td>
<td>236</td>
</tr>
<tr>
<td>configuration checklist (table)</td>
<td>233</td>
</tr>
<tr>
<td>described</td>
<td>233, 234</td>
</tr>
<tr>
<td>configure phone features</td>
<td>541</td>
</tr>
<tr>
<td>end</td>
<td>233, 235, 237</td>
</tr>
<tr>
<td>associating devices</td>
<td>237</td>
</tr>
<tr>
<td>configuration checklist (table)</td>
<td>233</td>
</tr>
<tr>
<td>described</td>
<td>233, 235</td>
</tr>
<tr>
<td>user alert, avoiding</td>
<td>299</td>
</tr>
<tr>
<td>user directory</td>
<td>233, 238</td>
</tr>
<tr>
<td>configuration checklist (table)</td>
<td>233</td>
</tr>
<tr>
<td>extension mobility</td>
<td>238</td>
</tr>
<tr>
<td>user groups</td>
<td>15, 25, 26, 582</td>
</tr>
<tr>
<td>CTI</td>
<td>582</td>
</tr>
<tr>
<td>described</td>
<td>15, 25</td>
</tr>
<tr>
<td>enterprise parameters</td>
<td>26</td>
</tr>
<tr>
<td>overview</td>
<td>15</td>
</tr>
<tr>
<td>user licenses</td>
<td>479</td>
</tr>
<tr>
<td>third-party SIP endpoints</td>
<td>479</td>
</tr>
<tr>
<td>user management, CTI</td>
<td>582</td>
</tr>
<tr>
<td>user options</td>
<td>541</td>
</tr>
<tr>
<td>Cisco Unified CM User Options</td>
<td>541</td>
</tr>
<tr>
<td>user profiles</td>
<td>236</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>V</td>
<td>421</td>
</tr>
<tr>
<td>V.150.1</td>
<td>421</td>
</tr>
<tr>
<td>MoIP support over secured SIP trunks</td>
<td>421</td>
</tr>
<tr>
<td>video</td>
<td>267, 543, 544, 545, 546, 547, 549, 555, 556, 558, 564, 570, 571, 574, 575</td>
</tr>
<tr>
<td>alternate routing</td>
<td>570</td>
</tr>
<tr>
<td>and Serviceability</td>
<td>574</td>
</tr>
<tr>
<td>bandwidth management</td>
<td>568</td>
</tr>
<tr>
<td>bridge counters</td>
<td>575</td>
</tr>
<tr>
<td>call details records</td>
<td>575</td>
</tr>
<tr>
<td>calling routing</td>
<td>571</td>
</tr>
<tr>
<td>calls</td>
<td>545</td>
</tr>
<tr>
<td>codecs</td>
<td>546</td>
</tr>
<tr>
<td>conference control</td>
<td>571</td>
</tr>
<tr>
<td>conference devices</td>
<td>267</td>
</tr>
<tr>
<td>configuration checklist (table)</td>
<td>543</td>
</tr>
<tr>
<td>configuring SIP trunk for calls</td>
<td>556</td>
</tr>
<tr>
<td>DSCP marking</td>
<td>570</td>
</tr>
<tr>
<td>gateway timer parameter</td>
<td>571</td>
</tr>
<tr>
<td>H.323</td>
<td>549</td>
</tr>
<tr>
<td>network</td>
<td>547</td>
</tr>
<tr>
<td>network example (figure)</td>
<td>547</td>
</tr>
<tr>
<td>other configuration</td>
<td>570</td>
</tr>
<tr>
<td>performance monitoring counters</td>
<td>574</td>
</tr>
<tr>
<td>phone configuration</td>
<td>570</td>
</tr>
</tbody>
</table>
video (continued)
  RSVP support 569
  SIP 556
  Skinny Client Control Protocol 555
  Skinny Client Control Protocol bridging 555
  telephony 544
  trunk interaction with H.323 client 571
  understanding 543
video phones 462
  Cisco Unified IP Phone 7985 462
viewing held calls on shared lines 193
voice codecs 37
  bandwidth used per call (table) 37
  G.711 37
  G.723 37
  G.729 37
  GSM 37
  supported by Cisco Unified Communications Manager 37
  wideband 37
voice compression 305
voice gateways 357
  gateways 357
voice mail 315, 316, 317, 318, 319, 321, 322, 325, 326, 540
  access 316
    directly connected 316
    overview 316
  call forwarding 321
    in multiple systems 321
    intercluster trunk, example 321
    intracluster trunk, examples 321
  call transfer 322
  configuring messages button 540
voice mail (continued)
  connectivity 315
    to Cisco Unified Communications Manager 315
  gateway-based 316
  interfaces 315
    intercluster 315
    overview 315
  PSTN gateway 315
  Skinny Protocol 315
  message waiting configuration 318
  message waiting indication 318
  pilot numbers 317
  prime line support for 319
  profiles 317
  SMDI 325, 326
    configuration checklist (table) 325
    integration 325
    requirements for integration 326
voice messaging 315
  voice mail 315
  voice quality 65
  VPN client 537
    described 537
W
  wideband 37
  wildcards 157, 166
    described (table) 166
    for hunt pilots 166
    for route patterns 166
    using @ in route patterns 157