CONTENTS

CHAPTER 1
IPv6 Introduction 1
  Documentation Changes 1
  IPv6 Deployment Overview 2
  Move Toward IPv6-Only Network 4
  Deployment Recommendations for Enterprise Networks 5
  Comparison of IPv4 and IPv6 6
    Why Deploy IPv6? 6
    Advantages of IPv6 Over IPv4 7

CHAPTER 2
IPv6 Basics 9
  IPv6 Basics Overview 9
  IPv6 Addressing 9
  IPv6 Unicast Addresses: Network and Host IDs 10
  Types of IPv6 Addresses 11
    Address Scopes 11
    Global Unicast Addresses 11
    Unique Local Unicast Addresses 12
    Link Local Unicast Addresses 13
  IPv6 Multicast Addresses 13
  Address Assignment for IPv6 Devices 14
    Manual Configuration 14
  IPv6 Stateless Address Auto-Configuration (RFC2462) 15
  DHCP for IPv6 15
    Stateless DHCP 16
    Stateful DHCP 16
  IPv6 Address Assignment Table 16

LAN Infrastructure 50
  General IPv6 LAN Design Guidance 50
  IPv6 Design Guidance for Collaboration Campus Networks 50
  First-Hop Redundancy Protocols 51
Network Services 52
  IPv6 Domain Name System (DNS) 52
  Dynamic Host Configuration Protocol for IPv6 (DHCPv6) 52
  DHCP and IPv4-only or IPv6-only Phones 53
  DHCP Server Recommendations 53
  DHCP Relay Agent 53
  Cisco IOS DHCPv6 Server 53
  Example Configuration for a Cisco IOS IPv6 DHCP Server 54
  Trivial File Transfer Protocol (TFTP) 55
  Network Time Protocol (NTP) 55
WAN Infrastructure 56
  General IPv6 WAN Design Guidance 56
  IPv6 Design Guidance for Unified Communications WAN Infrastructures 56
Call Admission Control 57
IPv6 Bandwidth Provisioning 58
  IPv6 Voice Bearer Traffic 59
  IPv6 Bandwidth Calculations 59
  Compressed RTP (cRTP) 60
  Call Control Traffic Provisioning 61
  RSVP 62
  WLAN 62
Network Management 62
  Cisco Prime Collaboration 62

CHAPTER 6 Gateways 63
  Gateways Overview 63

CHAPTER 7 Trunks 65
  Trunks Overview 65
  IPv6 SIP Trunks Configuration 66
Common Device Configuration Settings for SIP Trunks 66
  SIP Trunk IP Addressing Mode 66
  SIP Trunk IP Addressing Mode Preference for Signaling 67
Alternative Network Address Types (ANAT) 68
Recommended IPv6 SIP Trunk Configurations and Associated Call Flows 69
  Early Offer and SIP Trunk Calls 70
  Delayed Offer and SIP Trunks 70
  Unified CM SIP Trunk Signaling 71
    IP Addressing Version Used for SIP Signaling for Outbound 71
    IP Addressing Version Used for SIP Signaling for Inbound 71
Media Address Selection for Calls over Dual-Stack SIP Trunks (For DoD Networks Only) 72
  Media Selection for Outbound IPv6 Early Offer Calls Without ANAT 72
  Media Selection for Inbound Early Offer Calls Without ANAT (IPv6 Not Supported) 73
SIP Early Offer Calls with ANAT 75
  Alternative Network Address Types (ANAT) 75
  Media Selection for Outbound Early Offer Calls with ANAT 75
  Media Selection for Inbound Early Offer Calls With ANAT 77
SIP Trunks Using Delayed Offer 78
  Media Selection for Outbound Delayed Offer Calls Over Unified CM SIP Trunks Without ANAT 78
  Media Selection for Inbound Delayed Offer Calls Over Unified CM SIP Trunks Without ANAT 81
  Media Selection for Delayed Offer Calls Over Unified CM SIP Trunks With ANAT 82
  Media Selection for Outbound Delayed Offer Calls with ANAT 83
  Inbound Delayed Offer Calls with ANAT 85
  Inbound Delayed Offer Calls with ANAT and Supported: sdp-anat 85
  Inbound Delayed Offer Calls with ANAT and Require: sdp-anat 86

CHAPTER 8 Media Resources and Music on Hold 89
  Media Resources and Music on Hold Overview 89
  Media Termination Point (MTP) 89
  IPv6 and Other Media Resources 92

CHAPTER 9 Call Processing and Call Admission Control 95
Call Processing and Call Admission Control Overview 95

Call Processing 95

Enable Call Processing for IPv6 95

Configure IPv6 on Each Server in Cluster Using CLI 95

Configure Unified CM Server IPv6 Address Using GUI 96

Define Unified CM Server IPv6 Addresses 97

Cluster-Wide IPv6 Configuration 98

Unified CM Server Hardware Platforms 100

NIC Teaming for Network Fault Tolerance 100

Intra-Cluster Communications 100

TFTP Server 100

Unified CM CTI 100

Unified CM AXL/SOAP 101

SNMP 101

Cisco Collaboration Applications 101

Unified CM Platform Capacity Planning 101

Interoperability of Unified CM and Unified CM Express 101

Call Admission Control (CAC) 101

Call Admission Control with Unified Communications IPv6 Deployments 102

Locations-Based Call Counting Call Admission Control 103

Cisco Business Edition 103

CHAPTER 10

Dial Plan 105

Dial Plan Overview 105

IPv6 and Unified CM Dial Plans 106

SIP IPv6 Route Patterns 106

Path Selection Considerations for IPv6 Calls 108

Call Routing in Cisco IOS IPv6 Dial Peers 108

Emergency Services 108

CHAPTER 11

Applications 111

Applications Overview 111

CHAPTER 12

IP Video Telephony 115
IP Video Telephony Overview 115

CHAPTER 13  IP Telephony Migration Options 117
IP Telephony Migration Options Overview 117

CHAPTER 14  Security 119
Security Overview 119
Privacy and Encryption for IPv6 Voice Signaling and Media 119
Encrypted Media and MTPs Between IPv4 and IPv6 120
CAPF and CTL 121
IPv6 Collaboration Traffic and Firewalls 121
Cisco Unified Border Element 122
Security and IPv6 Traffic 122

CHAPTER 15  Collaboration Endpoints 123
IPv6 Capabilities of Collaboration Endpoints 123
IPv6 Support on Cisco IP Phones 123
Common Device Configuration Profile 124
Default Common Device Configuration Profile 126
Other IP Phone Functions 126
IPv6-Only Phones 127

CHAPTER 16  Appendix 129
Product Configuration Resources for IPv6 129
Document Direction 130
Deprecation of ANAT SIP SDP Attributes 131
CHAPTER 1

IPv6 Introduction

- Documentation Changes, on page 1
- IPv6 Deployment Overview, on page 2
- Move Toward IPv6-Only Network, on page 4
- Deployment Recommendations for Enterprise Networks, on page 5
- Comparison of IPv4 and IPv6, on page 6

Documentation Changes

Table 1: Documentation Changes

<table>
<thead>
<tr>
<th>Date</th>
<th>Change</th>
<th>Link to Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>April 10, 2019</td>
<td>Changed book title to 12.x to include Cisco Collaboration System Release 12.5.</td>
<td></td>
</tr>
</tbody>
</table>
## IPv6 Deployment Overview

This document describes our recommendations on how to transition your Cisco Collaboration network design to use IPv6 in a dual-stack (IPv4 and IPv6) environment.

This document does not describe how to implement IPv6 in the campus and WAN, but does refer you to other documents for those details. It is assumed that data IPv6 desktop services are deployed first, for example internet access when Collaboration IPv6 upgrade is initiated in a dual-stack mode.

<table>
<thead>
<tr>
<th>Date</th>
<th>Change</th>
<th>Link to Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>April 30, 2018</td>
<td>Updated overview based on Cisco Collaboration Systems Release (CSR) 12.1.</td>
<td>IPv6 Deployment Overview</td>
</tr>
<tr>
<td></td>
<td>Updated deployment gaps for CSR 12.1.</td>
<td>Deployment Recommendations for Enterprise Networks</td>
</tr>
<tr>
<td></td>
<td>Added a note about IPv6 multicast application.</td>
<td>IPv6 Multicast Addresses, on page 13</td>
</tr>
<tr>
<td></td>
<td>• Updated the recommended IPv6 addressing modes for CSR 12.1 endpoints.</td>
<td>IP Addressing Modes</td>
</tr>
<tr>
<td></td>
<td>• Added Cisco Meeting Server and Cisco TelePresence Management Suite.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Updated the note for CSR 12.1.</td>
<td>IPv6 Bandwidth Provisioning</td>
</tr>
<tr>
<td></td>
<td>• Added Cisco Meeting Server and Cisco TelePresence Management Suite in Video Conferencing section.</td>
<td>Applications Overview</td>
</tr>
<tr>
<td></td>
<td>• Added Multistream video section.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Updated Unified CM IM and Presence Service section to include dual-stack.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Added:</td>
<td>Product Configuration Resources for IPv6</td>
</tr>
<tr>
<td></td>
<td>• Cisco TelePresence EX Series</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Cisco Meeting Server</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Cisco TelePresence Management Suite</td>
<td></td>
</tr>
</tbody>
</table>

---

**IPv6 Introduction**
**Application Server Addressing Mode**

All Collaborations applications servers are deployed in IPv4 and IPv6 stacks to support IPv4 or IPv6 devices and components.

**Branch Office Addressing Mode**

In Cisco Collaboration Systems Release (CSR) 12.1, a branch office can be in one of the following IP addressing modes. A cluster can support the following types of IP addressing modes and all can co-exist.

- Traditional IPv4-only configuration where the LAN is IPv4-only or dual-stack.
- IPv6-only configuration where the LAN is dual-stack.
- Dual-stack sites that support IPv4 stack or IPv6 stack devices, where the LAN is dual-stack.
- US Department of Defense (DoD) dual-stack based on session initiation protocol (SIP) session description protocol (SDP) Alternative Network Address Types (ANAT) (not recommended), where the LAN is dual-stack.

CSR 12.1 provides IPv6-only site or branch offices that can have the following components:

- Cisco 4000 Series Integrated Services Routers (ISR) Edge Routers
  - PSTN GW
  - SRST
  - Audio Conference
  - MTP
- Endpoints
  - Video TP CE (Cisco DX Series, Cisco TelePresence MX, SX, and EX and Series)
  - Cisco IP Phone 7800 and 8800 Series
  - Conference IP Phone (8832)
  - On-premise Cisco Jabber (Jabber)
  - ATA FAX

---

**Note**

Cisco Technical Assistance Center (TAC) supports only solution tested components.

We strongly recommend that you use this document with following guides that provide in-depth guidance on Collaboration deployments using IPv4:

Cisco Collaboration IPv6 transition follows the Cisco Preferred Architecture (PA) recommended deployment of IPv4 products:

- Cisco Unified Communications Manager (Unified CM) is the call control server.
- Cisco IP Phones, Jabber clients, and Cisco TelePresence video endpoints use SIP to register directly to Unified CM.
- Unified CM cluster’s failover mechanism provides endpoint registration redundancy. If a WAN failure occurs, and endpoints at remote locations cannot register to Unified CM, they use SRST functionality for local and PSTN calls. However, some services such as Jabber presence might not be available.

Note

As of Cisco Collaboration Systems Release (CSR) 12.0, some default settings have not been adjusted for IPv6-only as a default, so follow the directions in this guide to ensure that you use the recommended settings for IPv6 deployment. Also some labels in the Admin Configuration UI have not been updated, but changes are noted in this document. For example, the Allow Auto-Configuration for Phones label has not been updated to Allow Stateless Auto-Configuration for Phones.

<table>
<thead>
<tr>
<th>Common Device Configuration Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name*</td>
</tr>
<tr>
<td>Softkey Template</td>
</tr>
<tr>
<td>User Hold MOH Audio Source</td>
</tr>
<tr>
<td>Network Hold MOH Audio Source</td>
</tr>
<tr>
<td>User Locale</td>
</tr>
<tr>
<td>IP Addressing Mode*</td>
</tr>
<tr>
<td>IP Addressing Mode Preference for Signaling*</td>
</tr>
<tr>
<td>Use Trusted Relay Point</td>
</tr>
<tr>
<td>Use Intercompany Media Services (IMS) for Outbound Calls*</td>
</tr>
<tr>
<td>IPv6 for Phones</td>
</tr>
<tr>
<td>Allow Auto-Configuration for Phones*</td>
</tr>
<tr>
<td>Allow Duplicate Address Detection*</td>
</tr>
<tr>
<td>Accept Redirect Messages*</td>
</tr>
<tr>
<td>Reply Multicast Echo Request*</td>
</tr>
</tbody>
</table>

Move Toward IPv6-Only Network

In Cisco Collaboration Systems Release (CSR) 12.0, the deployment of IPv6-only stack devices reduces dependency on IPv4 addresses. For all applications servers, emphasis is given to the deployment of two stack (IPv4 and IPv6) applications servers. Two stack applications servers offer a greater degree of functionality and interoperability with existing traditional IPv4-only devices that may not support IPv6-only stack because they are not developed in the CSR 12.0.

The ultimate goal is for all collaboration endpoints, servers, and gateways to be configured as IPv6-only stack, meaning that they can provide collaboration functions without using any IPv4 addresses and they do not require IPv4 to IPv6 media interworking functions.
Table 2: Reduction in IPv4 Addresses

<table>
<thead>
<tr>
<th>Scale of Deployment (Endpoints)</th>
<th>Servers and Gateways (Dual-stack or IPv4)</th>
<th>IPv4 Addresses Before Deploying IPv6-only Endpoints</th>
<th>IPv4 Addresses After Deploying IPv6-only Endpoints</th>
<th>Percent Reduction in IPv4 Addresses</th>
</tr>
</thead>
<tbody>
<tr>
<td>500</td>
<td>6</td>
<td>506</td>
<td>6</td>
<td>98.8%</td>
</tr>
<tr>
<td>5,000</td>
<td>13</td>
<td>5,013</td>
<td>13</td>
<td>99.7%</td>
</tr>
<tr>
<td>10,000</td>
<td>25</td>
<td>10,025</td>
<td>25</td>
<td>99.8%</td>
</tr>
</tbody>
</table>

The scope of this document is limited to the solutions that were tested and approved by Cisco. Supported IPv4-only stack applications are limited to those stated in this document. It is assumed that IP phones and gateways are configured with either an IPv4-only stack or IPv6-only stack using SIP signaling. Supported application servers support IPv4-only and IPv6-only stacks (dual-stack). Any applications that we did not develop or test are not supported by Cisco TAC. In IPv6 supported network configurations, Skinny Client Control Protocol (SCCP) for IP phones, voice gateways (Cisco VG Series Gateways), and Cisco Unity Connection are not configured and not tested except for the use of media termination points (MTP) by Cisco Unified Communications Manager.

Deployment Recommendations for Enterprise Networks

IPv4-only stack or IPv6-only stack devices support:

- Single-site call processing deployments.
- Multi-site distributed call processing deployments.
- Multi-site deployments with centralized call processing.

To move toward an IPv6 deployment and reduce dependency on IPv4 addresses, we recommend that you deploy:

- IPv6-only stack SIP phones, SIP gateways, and SIP trunks.
- IPv4-only stack and IPv6-only stack (dual-stack) Cisco Unified Communications Manager (Unified CM) clusters and other application servers.

For SIP trunks, we do not recommend use of Alternative Network Address Types (ANAT). ANAT requires IPv4 addresses and does not mitigate IPv4 exhaustion in an IPv6 network. ANAT is applicable only to US Department of Defense (DoD) deployments with Joint Interoperability Test Command (JITC) certification. Also, the PSTN SIP trunk service provider does not support ANAT.
**CSR 12.1/12.0 Deployment Gaps**

When you transition from a traditional IPv4 network to an IPv6 dual-stack network deployment, the following functionality is not supported and is not tested.

- IPv6-only stack site or branch office (LAN)
- IPv6-only data center
- All IP phones with SCCP signaling
- Secure IP phones, CE endpoints, and gateways
- Applications based on ISR and ISR G2 Routers
- IP phone VPN
- IP phones with NTP
- Video conference deployment based on Cisco TelePresence Conductor, Cisco TelePresence MCU, and Cisco TelePresence Server
- Mobile Remote Access (MRA)
- Cisco Expressway MRA support
- Off-premise Cisco Jabber
- Cisco Meeting Server
- Cisco TelePresence Management Suite
- SCCP signaling configuration IP phones
- SIP with ANAT signaling configuration
- RSVP call admission control
- Cisco Spark Hybrid Services
- Third-party API products
- Media Gateway Control Protocol (MGCP) gateways
- Unified CM supported H.323 gateways
- Products that are End-of-Support

**Comparison of IPv4 and IPv6**

This section provides a brief description of the motivation behind deploying IPv6, and a summary comparison of IPv4 and IPv6.

**Why Deploy IPv6?**

The deployment of IPv6 is primarily driven by IPv4 address exhaustion. As the worldwide usage of IP networks increases, the number of applications, devices, and services requiring IP addresses is rapidly increasing.
According to the Internet Assigned Numbers Authority (IANA) and Regional Internet Registries, their pool of unallocated IPv4 addresses is exhausted. For example, all area wireless networks in the American Registry for Internet Numbers (ARIN) are IPv6-only stack.

Because the current IPv4 address space is unable to satisfy the potential huge increase in the number of users and the geographical needs of the Internet expansion, many companies are either migrating to or planning their migration to IPv6, which offers a virtually unlimited supply of IP addresses.

Transforming the Internet from IPv4 to IPv6 is likely to take several years. During this period, IPv4 will co-exist with and then gradually be replaced by IPv6.

**Advantages of IPv6 Over IPv4**

As a new version of the Internet Protocol, IPv6 provides the following advantages over IPv4:

- **Larger address space (Supported in Cisco Collaboration Systems Release (CSR) 12.0)**

  The main feature of IPv6 that is driving adoption today is the larger address space. Addresses in IPv6 are 128 bits long compared to 32 bits in IPv4. The larger address space avoids the potential exhaustion of the IPv4 address space without the need for network address translation (NAT) or other devices that break the end-to-end nature of Internet traffic. By avoiding the need for complex sub-netting schemes, IPv6 addressing schemes are easier to understand, making administration of medium and large networks simpler.

- **Address scopes (Supported in CSR 12.0)**

  IPv6 introduces the concept of address scopes. An address scope defines the region, or span, where an address can be defined as a unique identifier of an interface. These spans are the link, the site network, and the global network, corresponding to link-local, site-local (or unique local unicast), and global addresses.

- **Stateless Address Auto-Configuration (SLAAC) (Supported in CSR 12.0)**

  IPv6 hosts can be configured automatically when connected to a routed IPv6 network using ICMPv6 router discovery messages. Address reconfiguration is also simplified. If IPv6 auto-configuration is not suitable, a host can use stateful configuration (DHCPv6) or can be configured manually.

- **Multicast (Not supported in CSR 12.0)**

  Multicast is part of the base specifications in IPv6, unlike IPv4, where it was introduced later. Like IPv6 unicast addresses, the IPv6 multicast address range is much larger than that of IPv4. IPv6 does not have a link-local broadcast facility; the same effect can be achieved by multicasting to the all-hosts group address (FF02::1).

- **Streamlined header format and flow identification (Not supported in CSR 12.0)**

  The IPv6 header format reduces router processing overhead by using a fixed header length, performing fragmentation on hosts instead of routers, and using an improved header extension method and a new flow label to identify traffic flows requiring special treatment.

- **Mobile IPv6 (Not supported in CSR 12.0)**

  Mobile IPv6 allows a mobile node to change its locations and addresses, while maintaining a connection to a specific address that is always assigned to the mobile node and through which the mobile node is always reachable. Mobile IPv6 provides transport layer connection survivability when a node moves from one link to another by performing address maintenance for mobile nodes at the Internet layer.
Mobile IPv6 is not supported by Cisco IP Phones or other collaboration components.

- Network-layer security (Not supported)

IPsec, the protocol for IP network-layer encryption and authentication, is part of the base protocol suite in IPv6. This is unlike IPv4, where IPsec is optional. Because of its reduced payload and performance overhead, products use TLS and SRTP for authentication and encryption.

The following table summarizes the differences between IPv4 and IPv6 services.

Table 3: IPv4 and IPv6 Services

<table>
<thead>
<tr>
<th>IP Service</th>
<th>IPv4 Feature</th>
<th>IPv6 Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address range</td>
<td>32-bit, NAT</td>
<td>128-bit, multiple scopes</td>
</tr>
<tr>
<td>Auto-configuration</td>
<td>DHCP</td>
<td>Stateless, Easy Reconfiguration, DHCP</td>
</tr>
<tr>
<td>Routing</td>
<td>RIP, OSPFv2, IS-IS, EIGRP, MP-BGP</td>
<td>RIPng, OSPFv3, IS-IS, EIGRP, MP-BGP</td>
</tr>
<tr>
<td>IP Security</td>
<td>IPsec</td>
<td>IPsec</td>
</tr>
<tr>
<td>Mobility</td>
<td>Mobile IP</td>
<td>Mobile IP with direct routing</td>
</tr>
<tr>
<td>Quality of Service (QoS)</td>
<td>Differentiated Service, Integrated Service</td>
<td>Differentiated Service, Integrated Service</td>
</tr>
<tr>
<td>IP multicast</td>
<td>IGMP, PIM, and Multicast BGP</td>
<td>MLD, PIM, and Multicast BGP; Scope Identifier</td>
</tr>
</tbody>
</table>
IPv6 Basics

IPv6 Basics Overview

This chapter provides an introduction to the basics of IPv6 addressing, including the various address types, address assignment options, new DHCP features, and DNS. For further reading on IPv6, you can refer to the following documentation:


• Other Cisco online documentation at http://www.cisco.com/go/ipv6

IPv6 Addressing

An IPv6 address consists of 8 sets of 16-bit hexadecimal values separated by colons (:), totaling 128 bits in length. For example:

```
2001:0db8:1234:5678:9abc:def0:1234:5678
```

You can omit leading zeros. For consecutive zeros in contiguous blocks, you can use a double colon (::). Double colons can appear only once in the address.

For example, here is the complete address:

```
2001:0db8:0000:130F:0000:0000:087C:140B
```
IPv6 Unicast Addresses: Network and Host IDs

IPv6 unicast addresses generally use 64 bits for the network ID and 64 bits for the host ID.

Figure 1: Format for IPv6 Unicast Network ID and Host ID

The network ID is administratively assigned. The host ID is configured manually or auto-configured by any of the following methods:

- Using a randomly generated number.
- Using DHCPv6.
- Using the Extended Unique Identifier (EUI-64) format. We commonly use the EUI-64 host ID format for devices such as Cisco IP Phones, gateways, and routers. This format, as illustrated, expands the device interface 48-bit MAC address to 64 bits by inserting FFFE into the middle 16 bits.

Figure 2: Conversion of EUI-64 MAC Address to IPv6 Host Address Format
Types of IPv6 Addresses

As with IPv4, IPv6 addresses are assigned to interfaces. However, unlike IPv4, an IPv6 interface is expected to have multiple addresses. There are several types:

- **Unicast address**—Identifies a single node or interface. Traffic destined for a unicast address is forwarded to a single interface.

- **Multicast address**—Identifies a group of nodes or interfaces. Traffic destined for a multicast address is forwarded to all the nodes in the group.

- **Anycast address**—Identifies a group of nodes or interfaces. Traffic destined to an anycast address is forwarded to the nearest node in the group. An anycast address is essentially a unicast address assigned to multiple devices with a host ID = 0000:0000:0000:0000. (Anycast addresses are not widely used today.)

With IPv6, broadcast addresses are no longer used. Broadcast addresses are too resource intensive, so IPv6 uses multicast addresses instead.

Address Scopes

An address scope defines the region where an address can be defined as a unique identifier of an interface. These scopes or regions are the link, the site network, and the global network, corresponding to link-local, unique local unicast, and global addresses.

Global Unicast Addresses

Global unicast addresses are:

- Routable and reachable across the Internet.

- IPv6 addresses for widespread generic use.

- Structured as a hierarchy to allow address aggregation.

- Identified by their three high-level bits set to 001 (2000::/3).
The global routing prefix is assigned to a service provider by the Internet Assigned Numbers Authority (IANA). The site level aggregator (SLA), or subnet ID, is assigned to a customer by their service provider. The LAN ID represents individual networks within the customer site and is administered by the customer.

The Host or Interface ID has the same meaning for all unicast addresses. It is 64 bits long and is typically created by using the EUI-64 format.

Example:


Unique Local Unicast Addresses

Unique local unicast addresses are:

- Analogous to private IPv4 addresses (for example, 10.1.1.254)
- Used for local communications, inter-site VPNs, and so forth
- Not routable on the Internet (routing would require IPv6 NAT)

Global IDs do not have to be aggregated and are defined by the administrator of the local domain. Subnet IDs are also defined by the administrator of the local domain. Subnet IDs are typically defined using a hierarchical addressing plan to allow for route summarization.

The Host or Interface ID has the same meaning for all unicast addresses. It is 64 bits long and is typically created by using the EUI-64 format.
**Link Local Unicast Addresses**

Link local unicast addresses are:

- Mandatory addresses that are used exclusively for communication between two IPv6 devices on the same link.
- Automatically assigned by device when IPv6 is enabled.
- Not routable addresses. Their scope is link-specific only.
- Identified by the first 10 bits (FE80).

**Figure 5: Format of Link Local Unicast Address**

![Link Local Unicast Address Format](image)

The remaining 54 bits of the network ID could be zero or any manually configured value. The interface ID has the same meaning for all unicast addresses. It is 64 bits long and is typically created by using the EUI-64 format.

Example:

FD00:aaaa:bbbb:CCCC:0987:65FF:FE01:2345

**IPv6 Multicast Addresses**

IPv6 multicast addresses have an 8-bit prefix, FF00::/8 (1111 1111). The second octet defines the lifetime and scope of the multicast address.

**Figure 6: Multicast Address Format**

![Multicast Address Format](image)

Multicast addresses are always destination addresses. Multicast addresses are used for router solicitations (RS), router advertisements (RA), DHCPv6, multicast applications, and so forth.
**IPv6 Basics**

IPv6 clients do not require a default gateway configuration because routers are discovered using RSs and RAs.

*Note*

Table 4: Common Multicast Addresses

<table>
<thead>
<tr>
<th>Address</th>
<th>Scope</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>FF01::1</td>
<td>Node-local</td>
<td>Same node</td>
</tr>
<tr>
<td>FF02::1</td>
<td>Link-local</td>
<td>All nodes on a link</td>
</tr>
<tr>
<td>FF01::2</td>
<td>Node-local</td>
<td>Same router</td>
</tr>
<tr>
<td>FF02::2</td>
<td>Link-local</td>
<td>All routers on a link</td>
</tr>
<tr>
<td>FF05::2</td>
<td>Site-local</td>
<td>All routers on the Internet</td>
</tr>
<tr>
<td>FF02::1:FFxx:xxxx</td>
<td>Link-local</td>
<td>Solicited node</td>
</tr>
</tbody>
</table>

For more information on IPv6 multicast addresses, refer to the IANA documentation: [http://www.iana.org/assignments/ipv6-multicast-addresses](http://www.iana.org/assignments/ipv6-multicast-addresses).

*Note*

IPv6 multicast application is not developed in Collaboration products, and is not supported industry wide through service provider networks.

---

## Address Assignment for IPv6 Devices

Addresses can be assigned in the following ways:

- **Manual Configuration, on page 14**
- **IPv6 Stateless Address Auto-Configuration (RFC2462), on page 15**
- **DHCP for IPv6, on page 15**
  - **Stateless DHCP, on page 16**
  - **Stateful DHCP, on page 16**

### Manual Configuration

Because IPv6 addresses are so complex, you won’t want to configure many of them manually. There’s too much administrative overhead. But you might want static addresses for router interfaces and certain network resources.
**IPv6 Stateless Address Auto-Configuration (RFC2462)**

One of the easiest ways to assign IP addresses is to set up IPv6 Stateless address auto-configuration (SLAAC) on an IPv6 router.

The network administrator configures the router to send Router Advertisement (RA) announcements onto the link. Then the on-link connected IPv6 nodes configure themselves with an IPv6 address and routing parameters. They get the IPv6 network prefix from the link-local router's RAs. They create the IPv6 host ID by using the device's MAC address and the EUI-64 format for host IDs.

**DHCP for IPv6**

IPv6 devices use multicast to acquire IP addresses and to find DHCPv6 servers. The basic DHCPv6 client-server concept is similar to DHCP for IPv4. If a client wants to receive configuration parameters, it sends out a request on the attached local network to detect available DHCPv6 servers.

- The DHCPv6 client requests parameters from an available server. This is done using Solicit and Advertise message and well-known DHCPv6 multicast addresses.
- The server responds with the requested information in a Reply message. As with DHCPv4, DHCPv6 uses an architectural concept of "options" to carry more parameters and information within DHCPv6 messages.

*Figure 7: IPv6 DHCP Messages*

The DHCPv6 client knows whether to use DHCPv6 based upon the instruction from a router on its link-local network. The default gateway has two configurable bits in its Router Advertisement (RA) available for this purpose:

- O bit—When this bit is set, the client can use DHCPv6 to retrieve other configuration parameters (for example, TFTP server address or DNS server address) but not the client's IP address.
- M bit—When this bit is set, the client can use DHCPv6 to retrieve a managed IPv6 address and other configuration parameters from a DHCPv6 server.
Stateless DHCP

Stateless DHCPv6, which is specified by RFC3736, is a combination of Stateless address auto-configuration (SLAAC) and Dynamic Host Configuration Protocol (DHCP) for IPv6.

When a router sends an RA with the O bit set but does not set the M bit, the client can use SLAAC to obtain its IPv6 address and use DHCPv6 to obtain additional information, such as TFTP server address or DNS server address. This mechanism is known as Stateless DHCPv6 because the DHCPv6 server does not have to track the client address bindings.

Stateful DHCP

The Dynamic Host Configuration Protocol for IPv6 (DHCPv6) has been standardized by the Internet Engineering Task Force (IETF) through RFC3315. When a router sends an RA with the M bit set, this indicates that clients should use DHCP to obtain their IP addresses.

When the M bit is set, the setting of the O bit is irrelevant because the DHCP server also returns other configuration information together with the addresses. This mechanism is known as Stateful DHCPv6 because the DHCPv6 server tracks the client address bindings.

IPv6 Address Assignment Table

To automatically configure IP phones with IPv6 address assignment, use the following configuration in Unified CM and in router Routing Advertisement (RA).

<table>
<thead>
<tr>
<th>Address Assignment Method</th>
<th>Auto_config parameter on Unified CM</th>
<th>M-bit</th>
<th>O-bit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stateless DHCPv6 for IP Phone address, TFTP and DNS address</td>
<td>On</td>
<td>On</td>
<td>Off</td>
</tr>
<tr>
<td>IPv6 address Stateless prefix from RA and DHCP to pull TFTP and DNS address</td>
<td>On</td>
<td>Off</td>
<td>On</td>
</tr>
<tr>
<td>Invalid configuration</td>
<td>On</td>
<td>Off</td>
<td>Off</td>
</tr>
<tr>
<td>Stateless DHCPv6 for IP Phone address, TFTP and DNS address</td>
<td>Off</td>
<td>On</td>
<td>Off</td>
</tr>
<tr>
<td>Invalid configuration</td>
<td>Off</td>
<td>Off</td>
<td>On</td>
</tr>
<tr>
<td>Invalid configuration</td>
<td>Off</td>
<td>Off</td>
<td>Off</td>
</tr>
</tbody>
</table>
DNS for IPv6

Cisco Unified Communications Manager (Unified CM) uses DNS name-to-address resolution in the following cases:

- If DNS names are used to define Unified CM servers (not recommended)
- If SIP route patterns use DNS names to define destinations
- If SIP trunks use DNS names to define trunk destinations

For IPv6, the principles of DNS are the same as for IPv4, with the following exceptions:

- The nomenclature is different (AAAA records are used instead of A records).
- DNS name-to-address queries can return multiple IPv6 addresses.

### Table 6: Comparison of DNS Name and Address Resolution

<table>
<thead>
<tr>
<th>Resolution of:</th>
<th>IPv4</th>
<th>IPv6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname to IP address</td>
<td>A record: <a href="http://www.abc.test">www.abc.test</a> A 192.168.30.1</td>
<td>AAAA record: <a href="http://www.abc.test">www.abc.test</a> AAAA 2001:db8:C18:1::2</td>
</tr>
</tbody>
</table>
CHAPTER 3

IP Addressing Modes for Cisco Collaboration Products

- IP Addressing Modes, on page 19
- Recommended IPv6 Addressing Modes for CSR 12.1/12.0 Products, on page 20
- IPv6 Addressing in Cisco Collaboration Products, on page 26
- Configuration Parameters and Features for IPv6 in Unified CM, on page 28

IP Addressing Modes

IP addressing modes specify the types of addresses that a device can communicate with and understand. The following IP addressing modes are used as part of the Cisco Collaboration Systems Release (CSR) 12.0.

Table 7: IP Addressing Modes

<table>
<thead>
<tr>
<th>IP Addressing Mode</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4-only stack</td>
<td>Used for some endpoints and gateways.</td>
<td></td>
</tr>
<tr>
<td>IPv6-only stack</td>
<td>Used for some endpoints and gateways.</td>
<td></td>
</tr>
<tr>
<td>Two stacks: IPv4-only and IPv6-only</td>
<td>Used for applications servers, such as Cisco Unified Communications Manager, Cisco Unity Connection, Cisco Emergency Responder, and Cisco Unified Survivable Remote Site Telephony (Unified SRST). Also applicable to dual-stack endpoints that require ANAT support.</td>
<td>The session initiation protocol (SIP) session description protocol (SDP) alternative network address type (ANAT) attribute should not be configured to transition to IPv6-only. It is applicable for the DoD networks.</td>
</tr>
<tr>
<td>IP Addressing Mode</td>
<td>Description</td>
<td>Notes</td>
</tr>
<tr>
<td>-------------------</td>
<td>-------------</td>
<td>-------</td>
</tr>
<tr>
<td><strong>IPv6 Aware</strong></td>
<td>Used for applications servers that use IPv4 to transport IPv6 application information, such as the Cisco Prime Collaboration Provisioning module, Cisco Emergency Responder, and Unified CM.</td>
<td>IPv6 aware devices communicate with IPv4 addresses, but can receive and understand IPv6 addresses embedded in application protocol data units (PDUs).</td>
</tr>
<tr>
<td><strong>Dual-stack</strong></td>
<td>Used only for Cisco Unified IP Phones 6900 and 7900 Series for DoD networks. We do not recommend dual-stack for enterprise networks. It is applicable for the DoD network. Dual-stack endpoints require IPv4 and IPv6 addresses to support SIP SDP ANAT. These devices communicate with and understand both IPv4 and IPv6 addresses.</td>
<td>The ANAT SDP Grouping Framework should not be configured in Collaboration products. We are removing dual-stack support to follow IETF deprecation of RFC 4091 and 4092. Dual-stack implies, both IPv4 and IPv6 addresses are available to use for both signaling and media. For media, dual-stack devices can take full advantage of the fact that they support both IPv4 and IPv6 when they communicate to any other device. For signaling, the IP addressing mode is set to either IPv4 or IPv6 by the device configuration. However, this functionality prevents transition to an IPv6-only stack network. From CSR 12.0 onward, the term, dual-stack is applicable only for DoD network’s endpoint deployments.</td>
</tr>
</tbody>
</table>

### Recommended IPv6 Addressing Modes for CSR 12.1/12.0 Products

For Collaboration IPv6 implementations, we recommend that you configure:

- IPv6-only stack for endpoints and gateways where supported.
• IPv4-only and IPv6-only stack for application servers and interfaces where supported. Unified CM and other applications ensure interoperability with existing IPv4-only devices and applications.

The following tables illustrate the recommended SIP IP addressing modes for Cisco Collaboration Systems Release (CSR) 12.1/12.0 products. Any products not listed here should be configured in IPv4-only stack.

For a list of product configuration resources for IPv6, see Product Configuration Resources for IPv6, on page 129.

**Table 8: Recommended IPv6 Addressing Modes for CSR 12.1/12.0 Endpoints**

<table>
<thead>
<tr>
<th>Endpoint (SIP)</th>
<th>IPv4-only</th>
<th>IPv6-only</th>
<th>Two Stacks: IPv4 and IPv6</th>
<th>Solution Tested in CSR 12.1/12.0</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IP Phone 7811, 7821, 7841, 7861</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Cisco IP Phone 8811, 8841, 8845, 8851, 8861, 8865</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Cisco IP Conference Phone 7832</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Cisco IP Conference Phone 8832</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Cisco Jabber</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>IPv6-only is for on-premise Jabber desktop deployment. No ANAT.</td>
</tr>
<tr>
<td>Endpoint (SIP)</td>
<td>IPv4-only</td>
<td>IPv6-only</td>
<td>Two Stacks: IPv4 and IPv6</td>
<td>Solution Tested in CSR 12.1/12.0</td>
<td>Comments</td>
</tr>
<tr>
<td>-------------------------------------------------------------------------------</td>
<td>-----------</td>
<td>-----------</td>
<td>---------------------------</td>
<td>-----------------------------------</td>
<td>--------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Cisco DX70 and DX80, Cisco TelePresence MX Series, Cisco TelePresence SX Series (CE endpoints)</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Manual configuration only. DHCP IPv6 is not supported.</td>
</tr>
<tr>
<td>Cisco TelePresence System EX Series</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Upgrade to CE software.</td>
</tr>
<tr>
<td>Endpoint (SIP)</td>
<td>IPv4-only</td>
<td>IPv6-only</td>
<td>Two Stacks: IPv4 and IPv6</td>
<td>Solution Tested in CSR 12.1/12.0</td>
<td>Comments</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-----------</td>
<td>-----------</td>
<td>---------------------------</td>
<td>----------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>Wi-Fi enabled devices: Cisco IP Phone 8861, 8865</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Cisco IP Communicator</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Table 9: Recommended IPv6 Addressing Modes for CSR 12.1/12.0 Communication Gateways**

<table>
<thead>
<tr>
<th>Gateway</th>
<th>Applications</th>
<th>IPv4-only</th>
<th>IPv6-only</th>
<th>Two Stacks: IPv4 and IPv6</th>
<th>Solution Tested in CSR 12.1/12.0</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco 4000 Series Integrated Services Routers (ISR)</td>
<td>Includes the following Applications. Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Product required for IPv6 deployment.</td>
</tr>
<tr>
<td></td>
<td>IOS Gateways</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Unified SRST</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>CUBE</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Only ISR G2 tested.</td>
</tr>
<tr>
<td></td>
<td>MTP</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Only ISR 4000 tested.</td>
</tr>
<tr>
<td>Cisco 2900 and 3900 Series Integrated Services Routers (ISR)</td>
<td>Includes the following Applications. Yes, SIP</td>
<td>No</td>
<td>Yes</td>
<td>Only for Cisco Unified Border Element (CUBE)</td>
<td>Partial, Yes for CUBE</td>
<td>SCCP signaling is not supported. No ANAT.</td>
</tr>
<tr>
<td></td>
<td>IOS Gateways</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Unified SRST</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>CUBE</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>MTP</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Gateway</td>
<td>Applications</td>
<td>IPv4-only</td>
<td>IPv6-only</td>
<td>Two Stacks: IPv4 and IPv6</td>
<td>Solution Tested in CSR 12.1/12.0</td>
<td>Comments</td>
</tr>
<tr>
<td>---------</td>
<td>--------------</td>
<td>-----------</td>
<td>-----------</td>
<td>---------------------------</td>
<td>---------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>Cisco 2800 and 3800 Series Integrated Services Routers (ISR)</td>
<td>Includes the following Applications.</td>
<td>Yes, SIP</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>SCCP signaling is not supported.</td>
</tr>
<tr>
<td></td>
<td>IOS Gateways</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Unified SRST</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>CUBE</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>MTP</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Cisco AS5400 Series Universal Gateways</td>
<td>Yes, SIP</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>SCCP signaling is not supported.</td>
</tr>
<tr>
<td>Cisco VG Series Gateways</td>
<td>Yes, SIP</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>SCCP signaling is not supported.</td>
</tr>
<tr>
<td>Cisco ATA 190 Series Analog Telephone Adapters</td>
<td>Yes, SIP</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Fax support.</td>
</tr>
<tr>
<td>H.323 Gateways</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td></td>
<td>ISR G1 G2.</td>
</tr>
<tr>
<td>Media Gateway Control Protocol (MGCP) Gateways</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td></td>
<td>ISR G1 G2.</td>
</tr>
</tbody>
</table>

Table 10: Recommended IPv6 Addressing Modes for CSR 12.1/12.0 Applications and Interfaces

<table>
<thead>
<tr>
<th>Application or Interface</th>
<th>IPv4-only</th>
<th>IPv6-only</th>
<th>Two Stacks: IPv4 and IPv6</th>
<th>Solution Tested in CSR 12.1/12.0</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Unified Communications Manager (Unified CM)</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Product required for IPv6 deployment.</td>
</tr>
</tbody>
</table>
### IPv6 Deployment Guide for Cisco Collaboration Systems Release 12.x

#### Recommended IPv6 Addressing Modes for CSR 12.1/12.0 Products

<table>
<thead>
<tr>
<th>Application or Interface</th>
<th>IPv4-only</th>
<th>IPv6-only</th>
<th>Two Stacks: IPv4 and IPv6</th>
<th>Solution Tested in CSR 12.1/12.0</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Unified Communications Manager IM and Presence Service (IM and Presence Service)</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Product required for IPv6 deployment.</td>
</tr>
<tr>
<td>Cisco Unified Communications Manager Express (Unified CME)</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Cisco Unified Survivable Remote Site Telephony (Unified SRST)</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Product required for IPv6 deployment for ISR G3.</td>
</tr>
<tr>
<td>Cisco Unified Contact Center Enterprise (Unified CCE)</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td></td>
<td>For Agent IPv6-only stack, NAT64.</td>
</tr>
<tr>
<td>Cisco Unified Contact Center Express (Unified CCX)</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td></td>
<td>For Agent IPv6-only stack, NAT64.</td>
</tr>
<tr>
<td>Cisco Emergency Responder (Emergency Responder)</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cisco Unity Connection</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Cisco Meeting Server</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Cisco TelePresence Management Suite</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Cisco Unity Express</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>
IPv6 Addressing in Cisco Collaboration Products

As you design your network, you'll need information about the number of IPv6 addresses that the various products can support.

Cisco Unified Communications Manager and IPv6 Addresses

Each Cisco Media Convergence Server (MCS) can support the following addresses simultaneously:

- One IPv6 link local address (for example, FE80::987:65FF:FE01:2345)
- Either of the following:

<table>
<thead>
<tr>
<th>Application or Interface</th>
<th>IPv4-only</th>
<th>IPv6-only</th>
<th>Two Stacks: IPv4 and IPv6</th>
<th>Solution Tested in CSR 12.1/12.0</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>End-of-Sale: Cisco Unified MeetingPlace</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Cisco Prime Collaboration</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>By customer</td>
<td>Applicable to IOS Gateways, Unified SRST, CUBE.</td>
</tr>
<tr>
<td>Cisco Smart Software Licensing</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>By customer</td>
<td>Applicable to Unified CM, IM and Presence Service, Cisco Unity Connection.</td>
</tr>
<tr>
<td>LAN/WAN</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Dynamic Host Configuration Protocol (DHCP)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Domain Name System (DNS)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Directory LDAP</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>NAT64</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Except for Unified CCE and Unified CCX, which have internal NAT64.</td>
</tr>
</tbody>
</table>
• One IPv6 unique local address (ULA), for example:

FD00:AAAA:BBBB:CCCC:0987:65FF:FE01:2345

• One IPv6 global address (GA), for example:


• One IPv4 address

All IPv6 devices must have a link local address that is automatically created.

A unique local address is equivalent to a private address in IPv4 (for example, 10.10.10.1).

A global address is a globally unique public address.

---

**Note**

Your IPv6 administrator decides on the selection of the address type. To route traffic from devices using unique local addresses over a public network, IPv6 NAT is required to convert unique local addresses to global addresses. We have not solution tested and do not recommend an IPv6 NAT-based solution.

---

**Cisco IP Phones and IPv6 Addresses**

A Cisco IP Phone can support a combination of the following addresses:

• One IPv6 link local address (for example, FE80::987:65FF:FE01:2345)

• Multiple IPv6 unique local addresses (for example, FD00:AAAA:BBBB:CCCC:0987:65FF:FE01:2345)

• Multiple IPv6 global addresses (for example, 2001:0DB8:BBBB:CCCC:0987:65FF:FE01:2345)

• One IPv4 address

Cisco IP Phones must support one link local address and can support a combination of up to 20 global or unique local addresses. The IP phone can use only IPv6 highest address scopes that can be received (RFC 4193) (global address or unique local IPv6 addresses) to register to Unified CM. After registration, this IPv6 address is used for signaling and media.

The following characteristics also apply to IPv6 addresses on IP phones:

• A link local address is never sent to Cisco Unified Communications Manager as a signaling and media address.

• If the IP phone has both unique local and global addresses, the highest scoped global addresses take precedence over unique local addresses.

• If the IP phone has multiple unique local addresses or multiple global addresses, the first address configured is the one used for signaling and media.

The following priority order applies to IPv6 addresses configured on an IP phone:

1. Use the IPv6 address configured manually through the phone's user interface (UI).
2. If an IPv6 address has not been configured manually on the phone, use Stateful DHCPv6 to assign an IPv6 address for IP phone, TFTP, and DNS.

3. If a manually configured address or a Stateful DHCPv6 address is not available, but stateless auto-configuration (SLAAC) is enabled for the phone, then the phone uses SLAAC to create an IPv6 address.

Note: In Cisco Unified Communications Manager, SLAAC is On by default. With SLAAC, the phone uses the IPv6 network prefix advertised in the link local router's Router Advertisements (RAs). The phone creates the IPv6 host ID by using the phone's MAC address and the EUI-64 format for host IDs. If SLAAC is used, Stateless DHCP IPv6 provides IPv6 address for TFTP and DNS server.

Cisco IOS Devices and IPv6 Addresses

Each interface of a Cisco IOS device can support a combination of the following addresses:

- One IPv6 link local address, for example:
  
  FE80::987:65FF:FE01:2345

- Multiple IPv6 unique local addresses, for example:
  
  FD00:AAAA:BBBB:CCCC:0987:65FF:FE01:2345

- Multiple IPv6 global addresses, for example:
  

- Multiple IPv4 addresses

Cisco IOS media termination points (MTPs) are associated with the router's interface through the `scup local <interface>` command. The MTP inherits the IPv4 and IPv6 addresses of the interface.

Configuration Parameters and Features for IPv6 in Unified CM

These configuration parameters and features support IPv6 in Cisco Unified Communications Manager (Unified CM):

- Common device configuration for phones and trunks
  
  - IP addressing mode
  
  - IP addressing mode preference for signaling
  
  - Allow Stateless auto-configuration for phones

- Role of the media termination point (MTP) in IPv6-enabled Unified CM clusters
• Alternative Network Address Types (ANAT) for SIP trunks
• New enterprise parameters
• MTP selection

You can enable and configure IPv6 for an entire cluster and you can configure your IPv6 devices (as shown in Recommended IPv6 Addressing Modes for CSR 12.1/12.0 Products, on page 20) to use IPv6 for signaling and media.

Common Device Configuration

Rather than add IPv6 configuration parameters to specific IP phones and SIP trunks and phones, you can use Unified CM's common device configuration template. This template contains the IPv6-specific configuration parameters for IP phones and SIP trunks. You can create and associate multiple common device configuration profiles to IP phones and SIP trunks.

To find the template, choose Device > Device Settings > Common Device Configuration.

The profile contains this configuration information for IPv6:

• IP Addressing Mode
• IP Addressing Mode Preference for Signaling
• Allow (Stateless) Auto-Configuration for Phones

Default Common Device Configuration

There is no default common device configuration profile. Devices are initially set to <None>. If you enable IPv6 in the Unified CM cluster in this <None> configuration, then your IPv6 devices adopt the following settings:

• IP Addressing Mode = IPv4 and IPv6
• IP Addressing Mode Preference for Signaling = Use System Default
• Allow (Stateless) Auto-Configuration for Phones = Default

Note

For enterprise deployment models of CSR 12.0, you must configure IP Addressing Mode to IPv6.
IP Addressing Mode for IPv6 Phones

After you configure the common device configuration profile and assign it to your phones, the specified IP addressing modes will be applied. The IP addressing modes are:

- **IPv4 Only**—The phone acquires and uses only one IPv4 address for all signaling and media. If the phone acquired an IPv6 address previously, it releases the IPv6 address.

- **IPv6 Only**—The phone acquires and uses only one IPv6 address for all signaling and media. If the phone acquired an IPv4 address previously, it releases the IPv4 address.

- **IPv4 and IPv6** (Not applicable for CSR 12.0)—The phone acquires and uses one IPv4 address and one IPv6 address. It can use the appropriate address as required for media. It uses either the IPv4 address or the IPv6 address for call control signaling.
For enterprise deployment models of the CSR 12.0, **IPv4 and IPv6** is not applicable. You must configure **IPv6 Only** or **IPv4 Only** as recommended in Recommended IPv6 Addressing Modes for CSR 12.1/12.0 Products, on page 20.

**Figure 9: Setting the Phone IP Addressing Mode**

<table>
<thead>
<tr>
<th>Common Device Configuration Information</th>
<th>IPv4 and IPv6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name*</td>
<td>Standard User</td>
</tr>
<tr>
<td>Softkey Template</td>
<td>1-SampleAudioSource</td>
</tr>
<tr>
<td>User Hold MOH Audio Source</td>
<td>1-SampleAudioSource</td>
</tr>
<tr>
<td>Network Hold MOH Audio Source</td>
<td>English, United States</td>
</tr>
<tr>
<td>User Locale</td>
<td>IPv4 and IPv6</td>
</tr>
<tr>
<td>IP Addressing Mode*</td>
<td>IPv4 Only</td>
</tr>
<tr>
<td>IP Addressing Mode Preference for Signaling*</td>
<td>IPv6 Only</td>
</tr>
<tr>
<td>Use Trusted Relay Point</td>
<td>IPv4 and IPv6</td>
</tr>
<tr>
<td>Use Intercompany Media Services (IMS)</td>
<td>IPv4 and IPv6</td>
</tr>
<tr>
<td>for Outbound Calls* *</td>
<td>IPv4 and IPv6</td>
</tr>
<tr>
<td>IPv6 for Phones</td>
<td>IPv4 and IPv6</td>
</tr>
<tr>
<td>Allow Auto-Configuration for Phones*</td>
<td>On</td>
</tr>
<tr>
<td>Allow Duplicate Address Detection*</td>
<td>On</td>
</tr>
<tr>
<td>Accept Redirect Messages*</td>
<td>Off</td>
</tr>
<tr>
<td>Reply Multicast Echo Request*</td>
<td>Off</td>
</tr>
</tbody>
</table>

If IPv6 is enabled in the Unified CM cluster, the default phone setting for IP addressing mode is IPv6. IP phones should not be configured for **IPv4 and IPv6**, it should be configured for IPv6-only phones.

**Note**

We recommend **IPv6 Only** endpoints for the CSR 12.0 enterprise deployment as shown in Recommended IPv6 Addressing Modes for CSR 12.1/12.0 Products, on page 20.

**IP Addressing Modes for Media Streams Between Devices**

Depending on the devices that you have chosen and the configuration profiles that you have set up, you can potentially have an assortment of devices using IPv4 addresses or IPv6 addresses. For two devices (such as phones) that support mismatched addressing modes, an IP addressing version incompatibility exists when a device with an IPv4 address wants to establish a RTP voice stream with a device with an IPv6 address. To resolve this IP addressing incompatibility for media, Unified CM dynamically inserts a media termination point (MTP) to convert the media stream from IPv4 to IPv6 or conversely. For more information on how and when MTPs are used for IPv6 calls, see Media Resources and Music on Hold Overview, on page 89.

**IP Addressing Mode Preference for Signaling for Phones**

The phone IP Addressing Mode Preference for Signaling has three settings:

- **IPv4**—The phone uses its IPv4 address for call control signaling to Unified CM.
- **IPv6**—The phone uses its IPv6 address for call control signaling to Unified CM.
- **Use System Default**—The phone uses the cluster-wide setting for IP Addressing Mode for Signaling if it has an address of that type. At first glance, you might worry that a cluster-wide setting could lead to incompatibility issues: What if a phone is using an IPv4 address and it tries to set up a voice stream with a phone that is using an IPv6 address? Unified CM handles this situation dynamically. It inserts an MTP that converts the media stream from IPv4 to IPv6 and back again.

![Figure 10: Common Device Configuration Information: IP Addressing Mode Preference for Signaling](image)

Allow (Stateless) Auto-Configuration for Phones

You can allow phones to receive an IP address and other information automatically. Your options are partly dependent on how you configure the link local router.

![Figure 11: Common Device Configuration Information: Allow (Stateless) Auto-Configuration for Phones](image)

You have these options:
• **On**—The phone can use Stateless Address Auto-Configuration (SLAAC), if supported by the link local router's configuration. It depends on the O and M bits in the Router Advertisements (RAs).

  - If the O-bit is set—The router allows the phone to use SLAAC to acquire its IP address and to use the DHCP server to acquire other information (such as the TFTP server address and DNS server address). This is known as stateless DHCP IPv6.

  - If the M-bit is set—The router does not allow the phone to use SLAAC but allows it to use the DHCP server to acquire its IP address and other information. This is known as stateful DHCP.

  - If neither bit is set—The router allows the phone to use SLAAC to acquire an IP address but does not allow it to use DHCP for other information. You need to configure a TFTP server address through the phone’s user interface (UI). The phone uses this TFTP server to download its configuration file and register to Unified CM. We do not recommend this for a production environment.

• **Off**—The phone does not use SLAAC to acquire an IPv6 address. In this case, the phone should use stateful DHCPv6 to acquire an IPv6 address and TFTP server address.

• **Default**—The phone uses the cluster-wide enterprise parameter configuration value for Allow (Stateless) Auto-Configuration for Phones. If IPv6 is enabled in the Unified CM cluster, the phone's default setting for Allow (Stateless) Auto-Configuration for Phones is Default. If the IP phone supports IPv6-only, it adopts the cluster-wide setting for Allow (Stateless) Auto-Configuration for Phones, but all IPv4 phones ignore this setting.

### Common Device Profile Configuration for SIP Trunks

You can apply SIP trunk configuration settings through the Common Device Configuration profile that you create and assign to the IPv6-Only SIP trunk with ANAT disabled.

With IPv6 enabled and with IPv4 addresses defined on the Unified CM server, you can configure the SIP trunk to use either of these addresses as its source IP address for SIP signaling. The SIP trunk also listens for incoming SIP signaling on the configured incoming port number of the server's IPv4 or IPv6 address.

### IP Addressing Mode for SIP Trunks

The SIP trunk IP addressing mode has three settings:

• **IPv4 Only**—The SIP trunk uses the Unified CM IPv4 address for signaling and either an MTP or phone IPv4 address for media.

• **IPv6 Only**—The SIP trunk uses the IPv6 address for signaling and either an MTP or phone IPv6 address for media.

• **IPv4 and IPv6** (Not applicable for CSR 12.0.)—For signaling, the SIP trunk will use either the Unified CM IPv4 address or the Unified CM IPv6 address. For media, the SIP trunk will use either an MTP IPv4 and/or IPv6 address or the phone IPv4 and/or IPv6 address.

If IPv6 is enabled in the Unified CM cluster, the default SIP trunk setting for the IP Addressing mode is IPv4 and IPv6. All IPv4 trunks (H.323 and MGCP) will ignore this setting.

We recommend setting the IP addressing mode for IPv6 SIP trunks to IPv4 or IPv6. The IPv6 Only setting is recommended and can be used in production environments.
For more information on these SIP trunk IP addressing modes, see SIP Trunks Using Delayed Offer, on page 78.

**IP Addressing Mode Preference for Signaling for SIP Trunks**

The SIP trunk IP Addressing Mode Preference for Signaling is used only for outbound calls. Unified CM listens for incoming SIP signaling on the configured incoming port number of the server's address.

The SIP trunk IP Addressing Mode Preference for Signaling has three settings:

- **IPv4**—The SIP trunk uses the Unified CM IPv4 address as its source address for SIP signaling.

- **IPv6**—The SIP trunk uses the Unified CM IPv6 address as its source address for SIP signaling.

**Note**

If IPv6 is enabled in the Unified CM cluster, this is the default SIP trunk setting for IP Addressing Mode Preference for Signaling. All IPv4 trunks ignore this setting.

- **Use System Default**—The SIP trunk uses the cluster-wide enterprise parameter configuration value for its IP addressing mode for signaling.

If IPv6 is enabled in the Unified CM cluster, the default SIP trunk setting for IP Addressing Mode Preference for Signaling is Use System Default. With this setting the SIP trunk will adopt the cluster-wide setting for IP Addressing Mode Preference for Signaling. All IPv4 trunks will ignore this setting.

The SIP trunk IP Addressing Mode Preference for Signaling is used only for outbound calls. Unified CM will listen for incoming SIP signaling on the configured incoming port number of the server's IPv4 and IPv6 address.

**Allow Auto-Configuration for Phones**

The parameter to Allow Auto-Configuration for Phones is not used by SIP trunks.

### Alternative Network Address Types

**Note**

Alternative Network Address Types (ANAT) is not applicable for CSR 12.0. ANAT is not applicable for all CSR 12.0 products. IPv4 to IPv6 media interworking is supported by Unified CM inserting MTPs.

ANAT is used in the SIP Offer and Answer exchange by dual-stack SIP trunks. ANAT allows these SIP devices to send both IPv4 and IPv6 addresses in the Session Description Protocol (SDP) body of a SIP Offer, and to return in the SDP body of the SIP Answer a preferred IP address (IPv4 or IPv6) with which to establish a voice connection.

We support ANAT over dual-stack (IPv4 and IPv6) SIP trunks. ANAT must be supported by both ends of the SIP trunk. You can enable ANAT by checking the Enable ANAT check box on the SIP profile associated with the SIP trunk. ANAT can be used with both Early Offer and Delayed Offer calls.
Enable ANAT only on SIP trunks with an IP addressing mode setting of **IPv4 and IPv6**.

Note

Before configuring the cluster-wide parameters in Unified CM, configure each server with an IPv6 address. For details on Unified CM IPv6 address configuration, see Configuring IPv6 in Cisco Unified CM, page A-1. In the Unified CM Administration interface, select **Enterprise Parameters > IPv6 Configuration Modes** to configure the following cluster-wide IPv6 settings for each Unified CM server:

- Enable IPv6
- IP Addressing Mode Preference for Media
- IP Addressing Mode Preference for Signaling
- Allow Auto-Configuration for Phones
Enable IPv6

Set this parameter to **True** to enable IPv6. False is the default setting.

**IP Addressing Mode Preference for Media**

IP Addressing Mode Preference for Media has two setting options:

- IPv4 (Default setting)
- IPv6 (**Recommended** setting)

The cluster-wide IP Addressing Mode Preference for Media is different than the device-level IP addressing mode. The cluster-wide IP Addressing Mode Preference for Media:

- Selects which IP addressing version will be used for media when a call is made between two dual-stack devices (Not applicable for the CSR 12.0 deployment)
- Is used when there is a mismatch in supported IP addressing versions between two devices. For example, if an IPv6-only device calls an IPv4-only device, an MTP must be inserted into the media path to convert from IPv4 to IPv6, and conversely.

Typically, both devices have MTP media resources available to them in their media resource group (MRG). The IP Addressing Mode Preference for Media is used to select which device's MTP is used to convert from IPv4 to IPv6 (and conversely) for the call, as follows:

- If the IP Addressing Mode Preference for Media is set to IPv4, the MTP associated with the IPv6-only device is selected, so that the longest call leg between the device and the MTP uses IPv4.
- If the IP Addressing Mode Preference for Media is set to IPv6, the MTP associated with the IPv4-only device is selected, so that the longest call leg between the device and the MTP uses IPv6.
- If the preferred device’s MTP is not available, the other device's MTP is used.
- If no MTPs are available, the call fails.
MTP resource allocation is discussed in detail in Media Resources and Music on Hold, on page 89.

**IP Addressing Mode Preference for Signaling**

The cluster-wide setting for the IP Addressing Mode Preference for Signaling is used by devices whose IP Addressing Mode Preference for Signaling is set to *Use System Default*. The IP Addressing Mode Preference for Signaling has two setting options:

- IPv4 (Default setting)
- IPv6 (*Recommended* setting)

**Allow (Stateless) Auto-Configuration for Phones**

The cluster-wide setting to Allow (Stateless) Auto-Configuration for Phones is used by phones whose Allow (Stateless) Auto-Configuration for Phones parameter is set to Default. The parameter to Allow (Stateless) Auto-Configuration for Phones has two setting options:

- On (Default setting)
- Off

**IPv6 Address Configuration for Unified CM**

After you configure an IPv6 address for the Unified CM server, you must also configure this address in the Unified CM Administration graphical user interface. This IPv6 address is used in the device configuration files stored on the cluster's TFTP servers. IPv6 devices can use this address to register with Unified CM. A server name can also be used, but an IPv6 DNS server is required to resolve this name to an IPv6 address.

*Figure 14:*

![IPv6 Deployment Guide for Cisco Collaboration Systems Release 12.x](image)
Collaboration Deployment Models for IPv6 Overview

This chapter describes the deployment models you can use with IPv6 in Cisco Collaboration networks. Cisco Unified Communications Manager (Unified CM) 12.0 supports the following traditional IPv4 deployment model examples:

- Single-site deployments
- Multi-site WAN deployments with distributed call processing
- Multi-site deployments with centralized call processing and Cisco Unified Survivable Remote Site Telephony (Unified SRST)

With all of these deployment models, IPv6 endpoints should be configured as IPv6 with a preference of IPv6 for signaling and media. This configuration maximizes the amount of IPv6 traffic with the use of media termination points (MTPs) for conversions between IPv4 and IPv6.

Single-Site Deployments

The single-site model for Cisco Collaboration consists of a call processing agent cluster located at a single site, or campus, with no telephony services provided over an IP WAN. An enterprise would typically deploy the single-site model over a LAN or metropolitan area network (MAN), which carries the voice, video, and IM traffic within the site. In this model, calls beyond the LAN or MAN use the public switched telephone network (PSTN).
The characteristics and benefits of the IPv6 single-site model are the same as for IPv4 single-site deployments, as described in the Cisco Collaboration Solution Reference Network Design (SRND), available at http://www.cisco.com/go/ucsrnd. The IPv6 single-site model includes the additional IPv6-only endpoints and dual stack application servers' product capabilities and features discussed throughout this document. As shown in Recommended IPv6 Addressing Modes for CSR 12.1/12.0 Products, on page 20, CSR 12.0 will not deploy dual stack endpoints.

**Best Practices for IPv6 Single-Site Deployments**

Single-site IPv6 deployments can contain a mixture of IPv4 and IPv6 devices. IPv6 phones can be configured as:

- IPv4-only
- IPv4 and IPv6 (Not Recommended)
- IPv6 only (Key feature of CSR 12.0)

Not applicable for the CSR 12.0 deployment:

- If IPv6 phones are configured as dual stack (IPv4 and IPv6), they should also be configured as follows:
  - To use IPv6 for signaling to Unified CM.
  - To prefer IPv6 over IPv4 for media.
One or more ISDN PSTN gateways can be deployed in a single-site deployment. If only one gateway is deployed, Cisco IOS ISR 4000 SIP gateway should be used.

**Note**

ISR 2G routers do not support IPv6-only gateways.

Both the Unified CM SIP trunk and Cisco IOS SIP gateway should be configured as follows:

- IPv6-only stack
- ANAT disabled for enterprise network
- To use IPv6 for signaling and media.

The Unified CM SIP trunk and the SIP gateway can be configured to use:

- SIP Delayed Offer (With **MTP Required** unchecked, although MTPs may be inserted dynamically for some calls for conversions between IPv4 and IPv6 addresses.)

**Note**

SIP Early Offer IPv6-only trunk is not supported in the CSR 12.0.

If a single IPv6 gateway is used and the cluster-wide preference for media is set to IPv6, an MTP is used for all calls to IPv4-only devices to convert from IPv4 to IPv6 protocol. If the widespread use of MTPs is not acceptable in the single-site deployment, configure two PSTN gateways instead of just one. Configure one as IPv4-only SIP gateway using SIP Delayed Offer as described above, and the other as a standard IPv6-only gateway. Calling search spaces and partitions can then be used to direct PSTN calls from IPv4-only and IPv6-only devices to their respective gateways.

For specific device configuration options and preferences, refer to the chapters on Trunks, on page 65, and Collaboration Endpoints, on page 123.

---

**The Campus LAN**

If the campus LAN uses Layer 2 switching only, enable Multicast Listener Discovery (MLD) in the campus switches if it is supported. Enabling MLD is not mandatory, but it is preferred because it reduces unwanted multicast traffic in the LAN.

If the campus LAN also includes Layer 3 routing devices, configure these devices to support dual-stack (IPv4 and IPv6) routing. IPv6-only stack is **not** supported in CSR 12.0.

**Note**

If a single PSTN gateway (as previously described) is used in this deployment model, then all Layer 3 LAN routing devices must be configured as dual-stack. If two gateways are used (one IPv6-only and one IPv4-only), then the portions of the network that contain IPv4-only devices do not have to be configured for dual-stack routing.
Multi-Site WAN Deployments with Distributed Call Processing

The model for a multi-site WAN deployment with distributed call processing consists of multiple independent sites, each with its own call processing cluster connected to an IP WAN that carries voice traffic between the distributed sites.

*Figure 16: Multi-Site Deployment with Distributed Call Processing*

Each site in the distributed call processing model can be one of the following:

- A single site with its own call processing agent, which can be either a:
  - Dual-stack (IPv4 and IPv6) Cisco Unified Communications Manager (Unified CM)
  - Standard (IPv4-only) Cisco Unified Communications Manager (Unified CM)
  - Standard (IPv4-only) Cisco Unified Communications Manager Express (Unified CME)
- Other IP PBX:
  - A standard (IPv4-only) centralized call processing site and all of its associated remote sites
A legacy PBX with Voice over IP (VoIP) gateway (IPv4-only or IPv6-only)

For dual-stack (IPv4 and IPv6) sites, the devices can be configured as either IPv4-only or IPv6-only. This configuration maximizes the amount of IPv6 traffic with the use of MTPs for conversions between IPv4 and IPv6 addresses.

The characteristics and benefits of an IPv6 multi-site WAN deployment with distributed call processing are the same as those for IPv4 multi-site WAN deployments with distributed call processing, as described in the Cisco Collaboration System Solution Reference Network Design (SRND), available at http://www.cisco.com/go/ucsrnd. The IPv6 multi-site model includes the additional IPv6-only and IPv6-only product capabilities and features discussed in this document.

Best Practices: Multi-Site WAN Deployments with Distributed Call Processing

A multi-site WAN deployment with distributed call processing has many of the same requirements as a single site. Follow the best practices from the single site model in addition to the ones listed here for the distributed call processing model.

IPv6 Unified CM clusters in multi-site WAN deployments with distributed call processing can use IPv6-only enabled SIP Delayed Offer intercluster trunks to connect to other IPv6 Unified CM clusters. However, for intercluster trunk connections to IPv4-only Unified CM clusters, we recommend using IPv4 SIP trunk delayed offer, not IPv6 intercluster trunks.

If IPv6-enabled SIP intercluster trunks are used, the WAN must support dual-stack (IPv4 and IPv6) routing.

Configure the Unified CM SIP intercluster trunks as follows:

- IPv6-only or IPv4-only (no ANAT is required).
- With ANAT disabled.
- To use IPv6 for signaling and media.

Configure the Unified CM SIP intercluster trunk to use:

- SIP Delayed Offer with MTP Required unchecked. Although MTPs may be inserted dynamically for some calls for conversions between IPv4 and IPv6 addresses.

SIP IPv6-only trunk Early Offer with MTP Required checked and used for every call is not supported.

For specific device configuration options and preferences, refer to Trunks, on page 65, and Collaboration Endpoints, on page 123.
Multi-Site Deployments with Centralized Call Processing and Unified SRST

In this call processing deployment model, endpoints can be located remotely from the call processing service (Unified CM cluster), across a QoS-enabled Wide Area Network (WAN). Due to the limited quantity of bandwidth available across the WAN, call admission control is required to manage the number of calls admitted on any given WAN link, to keep the load within the limits of the available bandwidth. On-net communication between the endpoints traverses either a LAN/MAN (when endpoints are located in the same site) or a WAN (when endpoints are located in different sites). Communication outside the enterprise goes over an external network such as the PSTN, through a gateway that is typically co-located with the endpoint.

The IP WAN also carries call control signaling between the central site and the remote sites. The following figure illustrates a typical centralized call processing deployment, with a Unified CM cluster as the call processing agent at the central site and an IP WAN to connect all the sites.
For IPv6-enabled multi-site centralized call processing deployments, the centralized Unified CM cluster is enabled for IPv4 and IPv6. Each site may be configured as dual-stacks or IPv4-only. For dual-stack (IPv4 and IPv6) sites, IPv6 devices should be configured as IPv6-only with a preference of IPv6 for signaling and media. This configuration maximizes the amount of IPv6 traffic using MTPs for conversions between IPv4 and IPv6 addresses.

The characteristics and benefits of an IPv6 multi-site centralized call processing deployment are the same as for IPv4 multi-site centralized call processing deployments, as described in the Cisco Collaboration System Solution Reference Network Design (SRND), available at http://www.cisco.com/go/ucsrnd. However, the IPv6 multi-site centralized call processing deployment model includes the additional IPv6-only product capabilities and features discussed in this document.
Best Practices: Multi-Site Deployments with Centralized Call Processing

IPv6 multi-site deployments with centralized call processing can contain sites with a mixture of traditional IPv4 and IPv6 devices. In each IPv6-enabled site, follow the best practices from the single-site model in addition to the ones listed here for the centralized call processing model.

You can configure IPv6-capable phones as:

- IPv4-only
- IPv4 and IPv6 (Recommended for DoD only.)
- IPv6-only (Recommended for production environments.)

The IP WAN in IPv6 multi-site deployments with centralized call processing must support dual-stack (IPv4 and IPv6) routing.

Unified SRST ISR 4000 routers at remote sites support IPv6-only or IPv4-only IP Phones in SRST mode. These SRST routers revert to original mode when the Unified CM cluster is restored. DoD supported dual-stack IP phones with ANAT are not supported in SRST mode and are not recommended for deployment at remote sites. They operate in IPv6-only mode.

Call Admission Control

For multi-site deployments with distributed or centralized call processing, use locations-based call admission control and a WAN based on either Multiprotocol Label Switching (MPLS) or a hub-and-spoke topology.


Note

MPLS design is supported, but is not committed and is not solution tested.

Intra-Cluster Communications

All intra-cluster server-to-server communications, such as Intra-Cluster Communication Signaling (ICCS) traffic, database traffic, and firewall management real-time traffic, use IPv4-only.

Clustering Over the WAN

We have tested clustering over the WAN with dual-stack Unified CM clusters through IPv6 SIP trunk interface by deploying SME or IPv6 SIP trunk directly.

Call Detail Records and Call Management Records

Call detail records (CDR) and call management records (CMR), when enabled, are collected by each subscriber server and are uploaded periodically to the publisher server, which stores the records in the CDR Analysis...
and Reporting (CAR) database. CDR and CMR collect and store both IPv4 and IPv6 addresses. These servers interface with IPv4 addresses that are IPv6-aware.
Network Infrastructure Overview

The requirements of the network infrastructure needed to build an IPv6 Collaboration system in an enterprise environment are very similar to those for an IPv4 Collaboration system. Unified Communications places strict requirements on IP packet loss, packet delay, and delay variation (or jitter). Therefore, you must enable most of the Quality of Service (QoS) mechanisms available on Cisco switches and routers throughout the network. For the same reasons, redundant devices and network links that provide quick convergence after network failures or topology changes are also important to ensure a highly available infrastructure. The Cisco Catalyst 6000 Series and Catalyst 4000 Series Switches use the same QoS architecture (DSCP) for IPv6 as they used for IPv4. With the exception of the Cisco Catalyst 3560 Series and 3750 Series Switches (which support QoS trust features only for IPv6), the same QoS mechanisms (such as classification, policing, queuing, and so forth) used for IPv4 Unified Communications traffic in Cisco switches and routers can also be applied to IPv6 Unified Communications traffic. Likewise, the redundant design and availability mechanisms for IPv4 networks are generally available in Cisco switches and routers for IPv6.


The following list summarizes the key network infrastructure recommendations for IPv6 Unified Communications networks:

- For Layer 2 switched networks, enable Multicast Listener Discovery (MLD) snooping, if possible, so that multicast traffic can be forwarded selectively to the ports that you want to receive the data.
- Layer 3 routed networks require a mechanism to transport IPv6 traffic. Native two stacks (IPv4 and IPv6) routing is recommended, although various other IPv6 tunneling mechanisms may also be used.
• Use Hot Standby Router Protocol (HRSP) or Gateway Load Balancing Protocol (GLBP) if those protocols are supported by your Layer 3 campus devices. Otherwise, use IPv6 Neighbor Unreachability Detection.

• IPv6 traffic uses larger headers, which you must factor into the bandwidth requirements for IPv6 traffic, especially in the WAN where bandwidth can be limited.

• For intercluster IPv6 traffic over IPv6-only or IPv4-only SIP intercluster trunks, use call admission control that is based on topology-unaware locations. (RSVP is not supported for IPv6). Topology-unaware call admission control requires a hub-and-spoke topology for the WAN, or a spokeless hub in the case of a Multiprotocol Label Switching (MPLS) virtual private network (VPN).

LAN Infrastructure

Campus LAN infrastructure design is extremely important for proper IP telephony operation on a converged network. Proper LAN infrastructure design requires following basic configuration and design best practices for deploying a highly available network. Furthermore, proper LAN infrastructure design requires deploying end-to-end QoS on the network. This section discusses specific IPv6 design guidance for campus networks. For general guidance on designing collaboration campus networks, refer to the Cisco Collaboration System Solution Reference Network Design (SRND), available at http://www.cisco.com/go/ucsrnd.

General IPv6 LAN Design Guidance

The following sources provide general guidance for designing IPv6 networks:

• Introduction to IPv6 in Cisco products
  http://www.cisco.com/go/ipv6

• Deploying IPv6 in Campus Networks

• Deploying IPv6 in Branch Networks

IPv6 Design Guidance for Collaboration Campus Networks

The following sections provide design guidance for deploying IPv6 in collaboration campus networks.

MLD and MLD Snooping in Switched Layer 2 IPv6 Campus Networks

IPv6 multicast routers use Multicast Listener Discovery (MLD) protocol to discover the presence of multicast listeners (nodes wishing to receive IPv6 multicast packets) on its directly attached links and to discover which multicast packets are of interest to neighboring nodes.

MLD snooping is similar to Internet Group Management Protocol (IGMP) snooping for IPv4. With MLD snooping, IPv6 multicast data is selectively forwarded to a list of ports that want to receive the data, instead of being flooded to all ports in a VLAN. This list is constructed by snooping IPv6 multicast control packets. If possible, enable Multicast Listener Discovery (MLD) snooping in your IPv6 LAN to reduce unwanted multicast traffic.
Layer 3 Campus Networks


Figure 18: Dual-Stack Routing in a Campus Network

First-Hop Redundancy Protocols

In the campus model, where the distribution switches are the L2/L3 boundary, they also act as the default gateway for the entire Layer 2 domain that they support. Some form of redundancy is required because this environment can be large and a considerable outage could occur if the device acting as the default gateway fails.

Hot Standby Router Protocol (HSRP) and Gateway Load Balancing Protocol (GLBP) first-hop redundancy protocols should be your first choice for high availability at the L2/L3 boundary and they also have useful features such as interface tracking, router prioritization, and preemption.

For IPv6 campus networks, the following Cisco IOS routing platforms support HSRP and GLBP first-hop redundancy protocols for IPv6:

- HSRP for IPv6 is supported on Cisco Catalyst 6500 Series Switches
- GLBP is supported on Cisco Catalyst 6500 Series Switches

Note

If your design does not permit the use of HSRP or GLBP, you can use Neighbor Unreachability Detection (NUD). However, due to its limitations in comparison to first-hop redundancy protocols, NUD is not recommended for collaboration IPv6 designs.

Neighbor Discovery for IPv6 (RFC 2461) implements the use of NUD. NUD is a mechanism that enables a host to determine whether a router (neighbor) in the host's default gateway list is unreachable. Hosts receive the NUD value (which is known as the "reachable time") from the routers on the local link through regularly sent router advertisements (RAs). The default reachable time is 30 seconds and is configurable. Neighbor Unreachability Detection can be used where first-hop redundancy protocols are not available; however, due to its limitations in comparison to first-hop redundancy protocols, Neighbor Unreachability Detection is not recommended for Unified Communications IPv6 designs.

Network Services

As with IPv4 collaboration systems, the deployment of an IPv6 collaboration system requires the coordinated design of a well-structured, highly available, and resilient network infrastructure. It also requires an integrated set of IPv6 network services including Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP), and Trivial File Transfer Protocol (TFTP). The deployment guidelines for these network services are generally the same as for IPv4 collaboration systems, but IPv6 network services are configured differently to support their IPv6 functionality. This section discusses the product and configuration details for IPv6 network services.

IPv6 Domain Name System (DNS)

As with IPv4, IPv6 DNS enables the mapping of hostnames and network services to IPv6 addresses within a network or networks. DNS servers deployed within a network provide a database that maps network services to hostnames and, in turn, hostnames to IPv6 addresses. Devices on the network can query the DNS server and receive IPv6 addresses for other devices in the network, facilitating communications between network devices. Complete reliance on a single network service such as DNS can introduce an element of risk when a critical collaboration system is deployed. If the DNS server becomes unavailable and a network device is relying on that server to provide a hostname-to-IP-address mapping, communications will fail. For this reason, in networks requiring high availability, we recommend that you do not rely on DNS name resolution for any communication between Cisco Unified Communications Manager (Unified CM) and the endpoints.

Unified CM can use DNS name-to-address resolution in the following situations:

- DNS names are used to define Unified CM servers and all other applications servers (Not recommended).
- SIP route patterns use DNS names to define destinations.
- SIP trunks use DNS names to define trunk destinations.

We recommend that you use Cisco Network Registrar (CNR) or Microsoft Windows server as an IPv4 and IPv6 DNS server in your collaboration network. Other DNS server products may be used, but we have not tested them.

Dynamic Host Configuration Protocol for IPv6 (DHCPv6)

IP phones can use DHCPv6 to obtain all of the initial configuration information that they need to register with Unified CM: an IPv6 address and an IPv6 TFTP server address.

In both IPv4 and IPv6 networks, DHCP eases the administrative burden of manually configuring each host with an IP address and other configuration information. DHCP also provides automatic reconfiguration of network addresses when devices are moved between subnets. We recommend Stateful DHCP host configuration for both IPv4 or IPv6 IP phones.
Unlike IPv4, which can use DHCP to inform a host of its default router, an IPv6 host uses Neighbor Discovery to find its local routers.

**Note**
IPv6 devices can use the DHCPv6 server in two ways:

- **Stateful DHCP** *(Recommended)* — Where the device retrieves its IP address and any other address information that it requires, such as TFTP server address, from the DHCP server.

- **Stateless DHCP** — Where the device uses stateless address auto-configuration (SLAAC) to obtain an IP address and uses the DHCP server to retrieve other information that it requires, such as TFTP server address.

### DHCP and IPv4-only or IPv6-only Phones

When the power is cycled on a dual-stack (IPv4 or IPv6) phone, it requests both IPv4 and IPv6 addresses and TFTP server information from its DHCP server(s). The phone then requests its configuration file from the TFTP server, which contains information about its IP Addressing Mode setting. If the IP Addressing Mode is set to IPv4 only, the IP phone releases its IPv6 address; and if the IP Addressing Mode is set to IPv6-only, the IP phone releases its IPv4 address. If the IP Addressing Mode is set to **IPv4 and IPv6**, the IP Phone retains both addresses and uses the setting of the IP Addressing Mode Preference for Signaling (IPv4 or IPv6) in the configuration file to select which address to use to register with and signal to its Unified CM server(s).

### DHCP Server Recommendations

We recommend that you use either a Cisco Network Registrar IPv4 and IPv6 DHCP server or a Cisco IOS IPv4 and IPv6 DHCP server in your collaboration network. Other DHCP server products from Microsoft Windows may be used, but we have not fully tested them.

### DHCP Relay Agent

A DHCP relay agent is used to relay messages between the client and server. DHCP relay agent operation is transparent to the client. A client locates a DHCP server using a reserved, link-scoped multicast address, which typically requires the DHCP client and the server to be attached to the same link. However, in some situations it is desirable to allow a DHCP client to send a message to a DHCP server that is not connected to the same link. Use the `dhcprelaydestination` command on your Cisco IOS router to forward DHCP client requests to a distant DHCP server.

The DHCP relay command is configured at the interface level, as follows:

- `dhcprelaydestination <ipv6-address> <interface-type interface-number>`

### Cisco IOS DHCPv6 Server

Example Configuration for a Cisco IOS IPv6 DHCP Server

The following example shows the configuration for a Cisco IOS IPv6 DHCP server.

! Activate DHCP Service on the IOS Device service dhcp
!
! Specify the name of this specific IPv6 DHCP pool, the address prefix and lifetime, the
! link address and
! vendor-specific option and sub option with TFTP server address(es) ipv6 dhcp pool
v6-CLUSTER-B
address prefix 2001:101:2:1::/64 lifetime 172800 86400 link-address 2001:101:2:1::/64
vendor-specific 9
suboption 1 address 2001:101:2::10 2001:101:2::11

Usage Guidelines

The ipv6 dhcp pool command enables the DHCPv6 pool configuration mode. The following configuration commands are available in this mode:

• **address prefix IPv6-prefix**
  This command sets an address prefix for address assignment. This address must be in hexadecimal form, using 16-bit values between colons.

• **lifetime t1 t2**
  This command sets a valid (t1) and a preferred (t2) time interval (in seconds) for the IPv6 address. The range is 5 to 4294967295 seconds. The valid default is 2 days, and the preferred default is 1 day. The valid lifetime must be greater than or equal to the preferred lifetime. Specify infinite for no time interval.

• **link-address IPv6-prefix**
  This command sets a link-address IPv6 prefix. When an address on the incoming interface or a link-address in the packet matches the specified IPv6-prefix, the server uses the configuration information pool. This address must be in hexadecimal form, using 16-bit values between colons.

• **vendor-specific**
  This command enables the DHCPv6 vendor-specific configuration mode. The following configuration command options are available in this mode:

  • **vendor-id**
    Enter a vendor-specific identification number. This number is the vendor IANA Private Enterprise Number. The range is 1 to 4294967295. Cisco's Enterprise Number (vendor ID) is 9.

  • **suboption number**
    This command sets the vendor-specific suboption number. The range is 1 to 65535. Enter an IPv6 address, ASCII text, or a hexadecimal string, as defined by the suboption parameters.

  • **TFTP Server Addresses option**
    Use suboption 1 for the TFTP Server Addresses option, and define the IPv6 addresses of the TFTP servers from which the client obtains its configuration file. List the TFTP server addresses in order of preference, and the client will attempt to obtain its configuration file from the TFTP servers in the order in which the addresses are listed.

  • **TFTP Service Name option**
    Use suboption 2 for the TFTP Service option that contains the name for the locally assigned TFTP Service. If no TFTP Server Addresses are provided in the DHCP response, this name is
resolved though a DNS service query. The name resolution may result in several addresses returned by the DNS server. This list contains the addresses of the TFTP servers from which the client obtains its configuration file. The TFTP server addresses are returned with an order of preference, and the client attempts to contact the target server with the lowest-numbered priority.

After you create the DHCPv6 configuration information pool, use the `ipv6 dhcp server` interface configuration command to associate the pool with a server on an interface. However, if you do not configure an information pool, you still need to use the `ipv6 dhcp server` interface configuration command to enable the DHCPv6 server function on an interface.

When you associate a DHCPv6 pool with an interface, only that pool services requests on the associated interface. The pool can also service other interfaces. If you do not associate a DHCPv6 pool with an interface, that pool can service requests on any interface.

Not using any IPv6 address prefix means that the pool returns only configured options.

The `link-address` keyword allows matching a link address without necessarily allocating an address. You can match the pool from multiple relays by using multiple `link-address` configuration commands inside a pool.

Because a longest match is performed on either the address pool information or the link information, you can configure one pool to allocate addresses and another pool on a subprefix that returns only configured options.

**Trivial File Transfer Protocol (TFTP)**

Within any Cisco Unified Communications Manager (Unified CM) system, endpoints such as IP phones rely on a TFTP-based process to acquire configuration files, software images, and other endpoint-specific information. The Cisco TFTP service is a file serving system that can run on one or more Unified CM servers. It builds configuration files and serves firmware files, ringer files, device configuration files, and so forth, to endpoints. To allow the TFTP server to serve files to devices using IPv6 signaling, the TFTP server inherits the IPv6 server address (the address configured through the server OS command line interface or the Cisco Unified Operating System Administration graphical user interface).

**Note** Peer-to-peer image file distribution is not supported with IPv6. However, a local IPv6 load server can be configured on IPv6 phones.

**Network Time Protocol (NTP)**

Network Time Protocol (NTP) enables network devices to synchronize their clocks to a network time server or network-capable clock. NTP is critical for ensuring that all devices in a network have the same time. When troubleshooting or managing a collaboration network, it is crucial to synchronize the time stamps within all error and security logs, traces, and system reports on devices throughout the network. This synchronization enables administrators to recreate network activities and behaviors based on a common timeline. Billing records and call detail records (CDRs) also require accurate synchronized time.
Unified CM NTP Time Synchronization

Unified CM supports NTP for IPv6. You can configure NTP v6 addresses through Unified CM Admin UI, BAT, and AXL. NTP v6 addresses are sent to a SIP Phone through phone configuration. In CSR 12.0, IP phones do not use IPv6 addresses configured for NTP server under Phone NTP References.

IP Phone NTP Time Synchronization

IP Phone NTP Time Synchronization for IPv6 is not supported.

Cisco IOS and CatOS NTP Time Synchronization

Cisco IOS and Cisco Catalyst OS (CatOS) do not support NTP for IPv6. If Cisco IOS NTP is used, IPv4 NTP should be used for clock synchronization.

WAN Infrastructure

Proper WAN infrastructure design is important for normal collaboration operation on a converged network. Proper infrastructure design requires following basic configuration and design best practices for deploying a WAN that is as highly available as possible and that provides guaranteed throughput. Furthermore, proper WAN infrastructure design requires deploying end-to-end QoS on all WAN links. This section discusses specific IPv6 design guidance for WAN infrastructures in collaboration networks. For general guidance on designing WAN infrastructures for collaboration deployments, refer to the Cisco Collaboration System Solution Reference Network Design (SRND), available at http://www.cisco.com/go/ucsrnd.

General IPv6 WAN Design Guidance

The following sources provide general guidance for designing IPv6 WAN infrastructures:

- Introduction to IPv6 in Cisco products
  

- Deploying IPv6 in Branch Networks
  

IPv6 Design Guidance for Unified Communications WAN Infrastructures

You may choose to run IPv6 Unified Communications traffic within your campus network only, in which case you can use standard IPv4 intercluster trunks between Unified CM clusters. If you wish to send IPv6 Unified Communications traffic between Unified CM clusters, then you must use IPv6 SIP intercluster trunks and an IPv6 WAN. Cisco recommends the deployment of both IPv4 and IPv6 routing protocols (a dual-stack WAN) for transporting IPv6 traffic over your WAN infrastructure.
The following deployment options are available for deploying IPv6 in a branch campus and across the WAN; however, we did not solution test these options.

- Run dual-stack (IPv4 and IPv6) routing protocols (Recommended).
- Deploy tunneling of IPv6 over IPv4 using:
  - Manually configured GRE tunnels
  - Manually configured IPv6 over IPv4 tunnels
  - Automatically configured IPv6-to-IPv4 (6 to 4) tunnels (RFC 3056)
- IPSEC can also be used to send IPv6 traffic securely in IPv4 tunnels for VPNs.

**Call Admission Control**

Unified CM supports only locations-based topology-unaware call admission control for IPv6. Resource Reservation Protocol (RSVP) cannot be used as a call admission control technique within the cluster or between clusters. Likewise, Unified CM IPv4 and IPv6 SIP trunks support only locations-based call admission control.

Topology-unaware call admission control requires a hub-and-spoke topology for the WAN, or a spokeless hub in the case of a Multiprotocol Label Switching (MPLS) virtual private network (VPN). This topology ensures that call admission control, provided by Unified CM's locations mechanism, works properly to track the bandwidth available between any two sites in the WAN.

Because using IPv6 requires 20 more bytes of data in its header than IPv4, an IPv6 call requires more bandwidth than a similar IPv4 call that uses the same type of codec and media payload.

To reserve and adjust the location-based bandwidth for a call that uses IPv6, Unified CM calculates the IP bandwidth that is needed for an IPv6 call using any supported codec. After the device contacts Unified CM for bandwidth reservation during the call setup, Unified CM identifies the IP version. If the call uses IPv6, Unified CM reserves the bandwidth for IPv6; and if the call uses IPv4, Unified CM reserves the bandwidth...
for IPv4. If both IP versions are supported by the devices, Unified CM initially reserves the IPv6 bandwidth and, if required, adjusts the bandwidth after media negotiation occurs. If Unified CM cannot identify the IP version used for the call, the call is extended over a SIP trunk using ANAT when applicable.

**Locations-Based Call-Counting Call Admission Control**

Unified CM also supports a type of locations-based, topology-unaware call admission control known as call counting. Less sophisticated than standard Unified CM locations-based call admission control, call counting uses a fixed bandwidth value for each voice and video call irrespective of the codec or actual bandwidth used.

For call-counting call admission control, the following default values are used for Layer 3 voice and video bandwidth when calculating the amount of available bandwidth at a location:

- A voice call = 102 kbps
- A video call = 500 kbps

Although call counting provides a simplified form of call admission control (CAC), it also has the disadvantage that bandwidth reserved for voice and video in the WAN might not be used efficiently.

To enable call counting in Unified CM Administration, select Service Parameters > Clusterwide Parameters (Call Admission Control). The default setting for Call Counting CAC Enabled is False. The voice and video bandwidth values for call counting are configurable.

*Figure 20: Configuring Call Counting for Call Admission Control*

---

**IPv6 Bandwidth Provisioning**

For general recommendations on bandwidth provisioning for collaboration traffic, refer to the bandwidth provisioning information in the Cisco Collaboration System Solution Reference Network Design (SRND), available at [http://www.cisco.com/go/ucsrnd](http://www.cisco.com/go/ucsrnd). However, when provisioning for IPv6 voice bearer traffic, you must consider the additional 20-byte overhead of the IPv6 header.

**Note**

In CSR 12.1, IPv6 video dual-stack ANAT traffic is not solution tested. To determine the bandwidth requirements for video flows, refer to the bandwidth provisioning information in the Cisco Collaboration System Solution Reference Network Design (SRND), available at [http://www.cisco.com/go/ucsrnd](http://www.cisco.com/go/ucsrnd).
IPv6 Voice Bearer Traffic

As illustrated in the following figure, a Voice-over-IPv6 (VoIPv6) packet consists of the voice payload, Real-Time Transport Protocol (RTP) header, User Datagram Protocol (UDP) header, IPv6 header and Layer 2 Link header. When Secure Real-Time Transport Protocol (SRTP) encryption is used, the voice payload for each packet increases by 4 bytes. The link header varies in size according to the Layer 2 media used.

IPv6 Bandwidth Calculations

To calculate the bandwidth consumed by VoIPv6 streams, add the packet payload and all headers (in bits), then multiplying by the packet rate per second, as follows:

- Layer 2 bandwidth in kbps = \( \left( \text{Packets per second} \times (\text{X bytes for voice payload} + 60 \text{ bytes for RTP/UDP/IP headers} + Y \text{ bytes for Layer 2 overhead}) \times 8 \text{ bits} \right) / 1000 \)
- Layer 3 bandwidth in kbps = \( \left( \text{Packets per second} \times (\text{X bytes for voice payload} + 60 \text{ bytes for RTP/UDP/IP headers}) \times 8 \text{ bits} \right) / 1000 \)
- Packets per second = \( \left[ \frac{1}{(\text{sampling rate in msec})} \right] \times 1000 \)
- Voice payload in bytes = \( \left( \frac{\text{codec bit rate in kbps} \times \text{sampling rate in msec}}{8} \right) \)

The following table details the Layer 3 bandwidth per VoIPv6 flow. It lists the bandwidth consumed by the voice payload and IPv6 header only, at a default packet rate of 50 packets per second (pps) and at a rate of 33.3 pps for both non-encrypted and encrypted payloads. It does not include Layer 2 header overhead. The codec sampling rate can be adjusted through the Unified CM Service Parameters menu.

<table>
<thead>
<tr>
<th>CODEC</th>
<th>Sampling Rate</th>
<th>Voice Payload in Bytes</th>
<th>Packets Per Second</th>
<th>Bandwidth Per Conversation</th>
</tr>
</thead>
<tbody>
<tr>
<td>G.711 and G.722-64k</td>
<td>20ms</td>
<td>160</td>
<td>50.0</td>
<td>88.0 kbps</td>
</tr>
<tr>
<td>G.711 and G.722-64k (SRTP)</td>
<td>20ms</td>
<td>164</td>
<td>50.0</td>
<td>89.6 kbps</td>
</tr>
<tr>
<td>G.711 and G.722-64k</td>
<td>30ms</td>
<td>240</td>
<td>33.3</td>
<td>79.2 kbps</td>
</tr>
<tr>
<td>G.711 and G.722-64k (SRTP)</td>
<td>30ms</td>
<td>244</td>
<td>33.3</td>
<td>81.0 kbps</td>
</tr>
</tbody>
</table>
Compressed RTP (cRTP)

Cisco IOS does not currently support Compressed RTP for IPv6.

A more accurate method of bandwidth provisioning is to include the Layer 2 headers in the bandwidth calculations. The following table lists the amount of bandwidth consumed by IPv6 voice traffic when the Layer 2 headers are included in the calculations.

<table>
<thead>
<tr>
<th>CODEC</th>
<th>Sampling Rate</th>
<th>Voice Payload in Bytes</th>
<th>Packets Per Second</th>
<th>Bandwidth Per Conversation</th>
</tr>
</thead>
<tbody>
<tr>
<td>iLBC</td>
<td>20ms</td>
<td>38</td>
<td>50.0</td>
<td>39.2 kbps</td>
</tr>
<tr>
<td>iLBC (SRTP)</td>
<td>20ms</td>
<td>42</td>
<td>50.0</td>
<td>40.8 kbps</td>
</tr>
<tr>
<td>iLBC</td>
<td>30ms</td>
<td>50</td>
<td>33.3</td>
<td>29.3 kbps</td>
</tr>
<tr>
<td>iLBC (SRTP)</td>
<td>30ms</td>
<td>54</td>
<td>33.3</td>
<td>30.4 kbps</td>
</tr>
<tr>
<td>G.729A</td>
<td>20ms</td>
<td>20</td>
<td>50.0</td>
<td>32.0 kbps</td>
</tr>
<tr>
<td>G.729A (SRTP)</td>
<td>20ms</td>
<td>24</td>
<td>50.0</td>
<td>33.6 kbps</td>
</tr>
<tr>
<td>G.729A</td>
<td>30ms</td>
<td>30</td>
<td>33.3</td>
<td>24.0 kbps</td>
</tr>
<tr>
<td>G.729A (SRTP)</td>
<td>30ms</td>
<td>34</td>
<td>33.3</td>
<td>25.0 kbps</td>
</tr>
</tbody>
</table>

Compressed RTP (cRTP)

Cisco IOS does not currently support Compressed RTP for IPv6.

A more accurate method of bandwidth provisioning is to include the Layer 2 headers in the bandwidth calculations. The following table lists the amount of bandwidth consumed by IPv6 voice traffic when the Layer 2 headers are included in the calculations.

**Table 12: Bandwidth Consumption with Layer 2 Headers Included**

<table>
<thead>
<tr>
<th>CODEC type and packet rate (packets per second)</th>
<th>Header Type and Size</th>
<th>Ethernet 14</th>
<th>PPP 6 Bytes</th>
<th>ATM 53-Byte Cells with a 48-Byte Payload</th>
<th>Frame Relay 4 Bytes</th>
<th>MLP 10 Bytes</th>
<th>MPLS 4 Bytes</th>
<th>WLAN 24 Bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>G.711 and G.722-64k at 50.0 pps</td>
<td>93.6 kbps</td>
<td>90.4 kbps</td>
<td>109.2 kbps</td>
<td>89.6 kbps</td>
<td>92 kbps</td>
<td>89.6 kbps</td>
<td>97.6 kbps</td>
<td></td>
</tr>
<tr>
<td>G.711 and G.722-64k (SRTP) at 50.0 pps</td>
<td>95.2 kbps</td>
<td>92 kbps</td>
<td>110.8 kbps</td>
<td>91.2 kbps</td>
<td>93.6 kbps</td>
<td>91.2 kbps</td>
<td>99.2 kbps</td>
<td></td>
</tr>
<tr>
<td>G.711 and G.722-64k at 33.3 pps</td>
<td>83.7 kbps</td>
<td>81.5 kbps</td>
<td>94.0 kbps</td>
<td>80.1 kbps</td>
<td>82.6 kbps</td>
<td>80.1 kbps</td>
<td>86.3 kbps</td>
<td></td>
</tr>
<tr>
<td>CODEC type and packet rate (packets per second)</td>
<td>Header Type and Size</td>
<td>Ethernet 14</td>
<td>PPP 6 Bytes</td>
<td>ATM 53-Byte Cells with a 48-Byte Payload</td>
<td>Frame Relay 4 Bytes</td>
<td>MLPPP 10 Bytes</td>
<td>MPLS 4 Bytes</td>
<td>WLAN 24 Bytes</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>----------------------</td>
<td>-------------</td>
<td>-------------</td>
<td>------------------------------------------</td>
<td>-----------------</td>
<td>---------------</td>
<td>-------------</td>
<td>--------------</td>
</tr>
<tr>
<td>G.711 and G.722-64k (SRTP) at 33.3 pps</td>
<td></td>
<td>84.7 kbps</td>
<td>82.6 kbps</td>
<td>95.1 kbps</td>
<td>82.1 kbps</td>
<td>83.7 kbps</td>
<td>82.1 kbps</td>
<td>87.4 kbps</td>
</tr>
<tr>
<td>iLBC at 50.0 pps</td>
<td></td>
<td>44.8 kbps</td>
<td>41.6 kbps</td>
<td>60.4 kbps</td>
<td>40.8 kbps</td>
<td>43.2 kbps</td>
<td>40.8 kbps</td>
<td>48.8 kbps</td>
</tr>
<tr>
<td>iLBC (SRTP) at 50.0 pps</td>
<td></td>
<td>46.4 kbps</td>
<td>43.2 kbps</td>
<td>62.0 kbps</td>
<td>42.4 kbps</td>
<td>44.8 kbps</td>
<td>42.4 kbps</td>
<td>50.4 kbps</td>
</tr>
<tr>
<td>iLBC at 33.3 pps</td>
<td></td>
<td>33.0 kbps</td>
<td>30.9 kbps</td>
<td>43.5 kbps</td>
<td>30.4 kbps</td>
<td>32.0 kbps</td>
<td>30.4 kbps</td>
<td>35.7 kbps</td>
</tr>
<tr>
<td>iLBC (SRTP) at 33.3 pps</td>
<td></td>
<td>34.1 kbps</td>
<td>32.0 kbps</td>
<td>44.5 kbps</td>
<td>31.5 kbps</td>
<td>33.1 kbps</td>
<td>31.5 kbps</td>
<td>36.8 kbps</td>
</tr>
<tr>
<td>G.729A at 50.0 pps</td>
<td></td>
<td>37.6 kbps</td>
<td>33.4 kbps</td>
<td>53.2 kbps</td>
<td>33.6 kbps</td>
<td>36.0 kbps</td>
<td>33.6 kbps</td>
<td>41.6 kbps</td>
</tr>
<tr>
<td>G.729A (SRTP) at 50.0 pps</td>
<td></td>
<td>39.2 kbps</td>
<td>36.0 kbps</td>
<td>54.8 kbps</td>
<td>35.2 kbps</td>
<td>37.6 kbps</td>
<td>35.2 kbps</td>
<td>43.2 kbps</td>
</tr>
<tr>
<td>G.729A at 33.3 pps</td>
<td></td>
<td>27.7 kbps</td>
<td>25.6 kbps</td>
<td>38.1 kbps</td>
<td>25.1 kbps</td>
<td>26.7 kbps</td>
<td>25.1 kbps</td>
<td>30.4 kbps</td>
</tr>
<tr>
<td>G.729A (SRTP) at 33.3 pps</td>
<td></td>
<td>28.8 kbps</td>
<td>26.7 kbps</td>
<td>39.2 kbps</td>
<td>26.1 kbps</td>
<td>27.8 kbps</td>
<td>26.1 kbps</td>
<td>31.5 kbps</td>
</tr>
</tbody>
</table>

**Call Control Traffic Provisioning**

Provisioning for call control traffic should not be a concern in a single-site Unified CM campus deployment. For multi-site WAN deployments with centralized or distributed call processing, you also need to consider bandwidth provisioning for inter-site signaling or intercluster trunk signaling traffic. For information on bandwidth provisioning for call control traffic over IPv4 trunks, refer to the Cisco Collaboration System Solution Reference Network Design (SRND), available at [http://www.cisco.com/go/ucsrnd](http://www.cisco.com/go/ucsrnd). For IPv6 signaling, add 10% to the bandwidth value calculated for call control traffic over IPv4.
RSVP

Resource Reservation Protocol (RSVP) call admission control is not supported for IPv6 calls. RSVP is not supported over Unified CM SIP trunks. Instead, use locations-based call admission control for intercluster trunks. We do **not** recommend the deployment of IPv6 in networks that use RSVP for call admission control.

WLAN

IPv6 is not supported by any Cisco wireless device. These devices support IPv4 only.

Network Management

This section discusses Cisco Prime Collaboration, a network management product.

Cisco Prime Collaboration

IPv6-aware Cisco Prime Collaboration provides simplified, unified management across voice and video collaboration networks. It offers automated provisioning, real-time monitoring, and proactive troubleshooting, plus long term trending and analytics—in one integrated product.

Cisco Prime Collaboration Advanced includes three separate modules:

- Provisioning (IPv6-aware and supports dual-stack and IPv6-only devices)
- Assurance (IPv4-only)
- Analytics (IPv4-only)

Cisco Prime Collaboration Standard includes a subset of the features available in the Provisioning and Assurance modules. The Analytics module and Cisco Prime Collaboration Contact Center Assurance are available as part of the Cisco Prime Collaboration Advanced offer only (IPv4-only).
Gateways

Gateways Overview

Gateways provide a number of methods for connecting an IP telephony network to the public switched telephone network (PSTN), legacy PBX systems, key systems, or analogue devices. Gateways range from specialized, entry-level and standalone voice gateways to high-end, feature-rich integrated routers and Cisco Catalyst gateways. For general guidance on gateway selection and features, refer to the Cisco Collaboration System Solution Reference Network Design (SRND), available at http://www.cisco.com/go/ucsrnd.

- IPv4-only stack supported gateways with SIP protocol as shown in: Recommended IPv6 Addressing Modes for CSR 12.1/12.0 Products, on page 20.

- Software and hardware media termination points (MTPs) for conversion between IPv4 and IPv6 use SCCP IPv4 signaling to Unified CM.

- All other gateway connections that use SCCP, H.323, and MGCP signaling protocols between Unified CM and the gateway have been deprecated.

- You can combine ISDN gateways, Unified SRST analog port, and MTP functionality on a single Cisco Integrated Services Router (ISR) 4000 platform. Unified SRST and CUBE cannot co-exist in the same ISR 4000 router.

- Cisco 2800 and 3800 Series Integrated Services Routers and Cisco VG Series Gateways must be configured as IPv4-only stack gateway. IPv6 functions will not be supported in CSR 12.0.
Trunks

- Trunks Overview, on page 65
- IPv6 SIP Trunks Configuration, on page 66
- Alternative Network Address Types (ANAT), on page 68
- Recommended IPv6 SIP Trunk Configurations and Associated Call Flows, on page 69
- Media Address Selection for Calls over Dual-Stack SIP Trunks (For DoD Networks Only), on page 72
- SIP Early Offer Calls with ANAT, on page 75
- SIP Trunks Using Delayed Offer, on page 78

Trunks Overview

Cisco Unified Communications Manager (Unified CM) supports several different types of IP trunks for connectivity with external devices:

- H.225 (H.323)
- SIP
- Intercluster trunks

Only SIP trunks and SIP intercluster trunks can support IPv6. This chapter describes the new IPv6 features and capabilities of these trunks. For information on the general capabilities and functions of Unified CM trunks, refer to the Cisco Collaboration System Solution Reference Network Design (SRND), available at http://www.cisco.com/go/ucsrnd.

There are several possible configurations for Unified CM SIP trunks:

- Inbound and outbound SIP Early Offer trunk calls
- Inbound and outbound SIP Early Offer trunk calls with Alternative Network Address Types (ANAT) enabled
- Inbound and outbound SIP Delayed Offer trunk calls (This chapter focuses on this recommended option)
- Inbound and outbound SIP Delayed Offer trunk calls with ANAT enabled
IPv6 SIP Trunks Configuration

To configure SIP trunks to gateways and Unified CM SIP intercluster trunks, select Devices > Trunks > SIP Trunk in Unified CM Administration.

The SIP trunk configuration settings discussed in this section are applied through the Common Device Configuration profile that is created and assigned to the SIP trunk (IP Addressing Mode and IP Addressing Mode Preference for Signaling), and through the SIP Profile configuration assigned to the SIP trunk (Enable ANAT should be disabled). The IPv4 to IPv6 media interworking is supported by Unified CM inserting MTPs.

**Figure 22: Trunk Configuration in Unified CM Administration**

**Common Device Configuration Settings for SIP Trunks**

This section describes the configuration settings for SIP trunks.

**SIP Trunk IP Addressing Mode**

You can configure the IP Addressing Mode to one of the following settings:

- IPv4
In this mode, the SIP trunk uses the Unified CM IPv4 address for signaling and either an MTP or phone IPv4 address for media.

- **IPv6**

In this mode, the SIP trunk uses the Unified CM IPv6 address for signaling and either an MTP or phone IPv6 address for media.

- **IPv4 and IPv6 (Not recommended, applicable to DoD network)**

The SIP trunk uses either the Unified CM IPv4 address or the Unified CM IPv6 address for signaling, and an MTP. We recommend IPv6 Only for production environments.

**Figure 23: IP Addressing Mode**

You can configure the IP Addressing Mode Preference for Signaling to one of the following settings:

- **IPv4**

In this mode, the SIP trunk uses the Unified CM IPv4 server address as its source address for SIP signaling.

- **IPv6**

In this mode, the SIP trunk uses the Unified CM IPv6 server address as its source address for SIP signaling.

- **Use System Default**

In this mode, the SIP trunk uses the cluster-wide Enterprise Parameter configuration value for its IP addressing mode for signaling.

If IPv6 is enabled in the Unified CM cluster, the default SIP trunk setting for the IP Addressing Mode for Signaling is **Use System Default**. With this setting, the SIP trunk adopts the cluster-wide setting for its IP addressing mode for signaling, if the trunk is configured with a destination address of that type. All IPv4 trunks ignore this setting.

---

**SIP Trunk IP Addressing Mode Preference for Signaling**

You can configure the IP Addressing Mode Preference for Signaling to one of the following settings:

- **IPv4**

In this mode, the SIP trunk uses the Unified CM IPv4 server address as its source address for SIP signaling.

- **IPv6**

In this mode, the SIP trunk uses the Unified CM IPv6 server address as its source address for SIP signaling.

- **Use System Default**

In this mode, the SIP trunk uses the cluster-wide Enterprise Parameter configuration value for its IP addressing mode for signaling.

If IPv6 is enabled in the Unified CM cluster, the default SIP trunk setting for the IP Addressing Mode for Signaling is **Use System Default**. With this setting, the SIP trunk adopts the cluster-wide setting for its IP addressing mode for signaling, if the trunk is configured with a destination address of that type. All IPv4 trunks ignore this setting.
The SIP trunk’s IP Addressing Mode Preference for Signaling is used only for outbound calls. Unified CM listens for incoming SIP signaling on both the IPv4 and IPv6 address.

**Figure 24: P Addressing Mode Preference for Signaling**

<table>
<thead>
<tr>
<th>Common Device Configuration Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name*</td>
</tr>
<tr>
<td>Softkey Template</td>
</tr>
<tr>
<td>User Hold MOH Audio Source</td>
</tr>
<tr>
<td>Network Hold MOH Audio Source</td>
</tr>
<tr>
<td>User Locale</td>
</tr>
<tr>
<td>IP Addressing Mode*</td>
</tr>
<tr>
<td>IP Addressing Mode Preference for Signaling*</td>
</tr>
<tr>
<td>☐ Use Trusted Relay Point</td>
</tr>
<tr>
<td>Use Intercompany Media Services (IMS) for Outbound Calls*</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IPv6 for Phones</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow Auto-Configuration for Phones*</td>
</tr>
<tr>
<td>Allow Duplicate Address Detection*</td>
</tr>
<tr>
<td>Accept Redirect Messages*</td>
</tr>
<tr>
<td>Reply Multicast Echo Request*</td>
</tr>
</tbody>
</table>

**Allow Auto-Configuration for Phones**

The setting of Allow Stateful Auto-Configuration for Phones is not used by SIP trunks.

## Alternative Network Address Types (ANAT)

ANAT is used in the SIP Offer and Answer exchange between dual-stack SIP trunks. ANAT allows SIP devices to send both IPv4 and IPv6 addresses in the Session Description Protocol (SDP) body of a SIP Offer, and to return in the SDP body of the SIP Answer a preferred IP address (IPv4 or IPv6) with which to establish a media connection.

We support ANAT over dual-stack (IPv4 and IPv4) SIP trunks. ANAT must be supported by both ends of the SIP trunk. To enable ANAT, check the Enable ANAT check box on the SIP Profile associated with the SIP trunk. ANAT can be used with both Early Offer and Delayed Offer calls.

**Note**

In CSR 12.0, ANAT is not configured and not supported by Unified CM and Unified SRST.

Enable ANAT only on SIP trunks with an IP Addressing Mode setting of *IPv4 and IPv6.*
Cluster-Wide Configuration Settings That Affect ANAT-Enabled SIP Trunk Calls

The cluster-wide setting *Addressing Mode Preference for Media* specifies which addressing version to use when a Unified CM SIP trunk with ANAT enabled receives an IPv6 and an IPv4 address in the SDP body of a SIP Offer. This cluster-wide setting also determines whether the phone's or trunk's MTP is selected when an MTP is dynamically inserted in a call through a SIP trunk.

**Recommended IPv6 SIP Trunk Configurations and Associated Call Flows**

How you configure your Unified CM IPv6 SIP trunk will, to some extent, depend upon the capabilities of the far-end SIP trunk device. Usually this far-end SIP trunk device is another Unified CM cluster, IPv6 SIP gateway, or third-party IPv6 SIP call agent.

Some general guidance on IPv6 SIP trunk configuration:

- IPv6 SIP trunks should be configured with an IP addressing mode of IPv4 and IPv6.
- If ANAT is required, then the trunk's IP addressing mode must be set to IPv4 and IPv6.
- If ANAT is required, both trunk devices must support it.
- SIP Early Offer and SIP Delayed Offer are supported, both in symmetric and asymmetric configurations, as follows:
  - Outbound and inbound SIP Early Offer *(Recommended)* option
  - Outbound and inbound SIP Delayed Offer
  - Outbound SIP Early Offer and inbound SIP Delayed Offer
  - Outbound SIP Delayed Offer and inbound SIP Early Offer
In CSR 12.0, SIP Early Offer does not support IPv6. CUBE or Unified SRST gateways will not support ANAT.

Note

Early Offer and SIP Trunk Calls

For all Unified CM SIP trunks, you must check the **MTP required** check box on the trunk configuration page to enable SIP Early Offer in IPv4 (IPv6 does not support Early Offer). When **MTP required** is checked, a media termination point (MTP) is used in the media path for all inbound and outbound calls. This statically assigned MTP affects all calls in the following ways:

- Because the MTP is placed in the media path for all calls, rather than having one call leg from the calling phone to the called phone, the insertion of the MTP creates two legs: one from the calling phone to the MTP, and the other from the MTP to the called phone. For signaling purposes, this can be considered to be two calls. The calling phone and MTP negotiate media capabilities (such as codec, IP addresses, and UDP port numbers to be used), as do the MTP and the called phone at the far end of the SIP trunk.

- The statically assigned MTP (**MTP required** checked) must be configured to use one codec type (G711 or G729). Assigning a single voice codec to this statically assigned MTP disables the use of the pass-through codec. This, in turn, prevents the negotiation of the pass-through codec that is required for video calls or encrypted calls. (T.38 fax calls are supported with statically assigned MTPs.) Therefore, if support for video or encryption is required over the SIP trunk, SIP Delayed Offer (no statically assigned MTP) must be used.

Note

The pass-through codec should be configured on all dynamically inserted MTPs. To enable the use of the pass-through codec, configure the MTP with both a standard codec and the pass-through codec.

If SIP Early Offer is required for dual-stack SIP Unified CM trunks, then you must configure the Cisco IOS MTP to use both an IPv6 and IPv4 address. For details, see Media Resources and Music on Hold Overview, on page 89.

Delayed Offer and SIP Trunks

Delayed Offer trunks do not have a statically assigned MTP and therefore MTP resources are not used for every call. For Delayed Offer calls, Unified CM attempts to set up the call using a single call leg between the calling and called device, and in doing so must consider the IP addressing mode configuration of both the Unified CM trunk and the IP phone registered with Unified CM. In certain calls where there are IP addressing mode mismatches between the Unified CM trunk and the registered phone, Unified CM dynamically inserts an MTP to resolve this mismatch. The pass-through codec is supported by this dynamically inserted MTP, and video calls and encrypted calls can be established with this MTP in the call path. The pass-through codec should be configured on all dynamically inserted MTPs. To enable the use of the pass-through codec, configure the MTP with both a standard codec and the pass-through codec.
Unified CM SIP Trunk Signaling

The following factors affect which IP addressing version is used for signaling on Unified CM SIP trunks:

- Call direction
- IP addressing mode of the trunk
- Configured destination addresses of the trunk
- Trunk's IP addressing mode preference for signaling
- Cluster-wide IP addressing mode preference for signaling

**IP Addressing Version Used for SIP Signaling for Outbound**

The IP addressing version for signaling is determined by the following factors, in the order listed here:

1. The IP Addressing Mode of the SIP trunk (IPv4 or IPv6)
2. The configured destination addresses of the SIP trunk (IPv4 or IPv6)
   - If only one destination address is configured (IPv4 or IPv6), the IP addressing version must match the IP Addressing Mode of the trunk. If these two values do not match, the SIP trunk connection is not established.
   - If two trunk destination addresses are configured (IPv4 and IPv6), then the IP addressing version is determined by the SIP trunk's IP Addressing Mode Preference for Signaling (IPv4, IPv6, or Use System Default). If the Use System Default setting is used, then the IP addressing version is determined by the cluster-wide IP Addressing Mode Preference for Signaling (IPv4 or IPv6).

**IP Addressing Version Used for SIP Signaling for Inbound**

For inbound calls, the IP addressing version used for signaling is based on the trunk destination addresses and port numbers configured in Unified CM. If the signaling source address and port number received from the calling device match a configured destination address and port number on the SIP trunk, then the signaling connection is established.

Unified CM provides the following configuration setting options for the SIP trunk destination address:

- One IPv4 address configured
- One IPv6 address configured
- One IPv4 and one IPv6 address configured (For DoD network only)

If IPv6 is enabled in the cluster, Unified CM servers listen for incoming SIP trunk calls destined to their configured IPv4 and IPv6 addresses and source port number.
Media Address Selection for Calls over Dual-Stack SIP Trunks (For DoD Networks Only)

Many configuration options are possible for SIP trunks. Trunks may be single or dual stack, have ANAT enabled or disabled, and use SIP Early Offer or SIP Delayed Offer. This chapter, while not exhaustive, discusses the significant configuration options and their outcomes in terms of the addresses that are exchanged and used for media. Early Offer call scenarios are considered first, followed by Delayed Offer call scenarios.

Depending on the call scenario, media address selection for calls over dual-stack SIP trunks can be based on:

- Call direction
- Whether Delayed Offer or Early Offer is used
- The IP Addressing Mode of the trunk
- The cluster-wide IP Addressing Mode Preference for Media
- The IP Addressing Mode of the phone

The remaining sections of this chapter review media selection for the following Unified CM call flows:

- SIP Early Offer calls
  - Outbound Early Offer calls without ANAT
  - Inbound Early Offer calls without ANAT
  - Outbound Early Offer calls with ANAT
  - Inbound Early Offer calls with ANAT

- SIP Delayed Offer calls
  - Outbound Delayed Offer calls without ANAT
  - Inbound Delayed Offer calls without ANAT
  - Outbound Delayed Offer calls with ANAT
  - Inbound Delayed Offer calls with ANAT

Media Selection for Outbound IPv6 Early Offer Calls Without ANAT

This is not supported in CSR 12.0
SIP Early Offer calls involve two call legs: one from the phone to trunk MTP, and the other from the trunk MTP to the SIP voice gateway. The Cisco IOS MTP is configured to support both IPv4 and IPv6 addresses. ANAT has not been enabled on the SIP trunk in the following figure, so as with a standard SIP trunk, only a single IP addressing version is exchanged.

**Figure 26: Media Selection on Unified CM SIP Trunks for Outbound Early Offer Calls Without ANAT**

Call Leg from Phone to Trunk MTP: Standard Unified CM In-Cluster Negotiation

The MTP is dual-stacked and can match the media addressing type of the phone if it is set to IPv4-only or IPv6-only. If the phone is also dual-stacked, the cluster-wide IP Addressing Mode Preference for Media (IPv4 or IPv6) determines which IP addressing version is used for media.

Call Leg from MTP Trunk to Voice Gateway: ANAT Not Enabled, and One Media Address Is Sent in SDP (IPv4 or IPv6)

For outbound Early Offer calls where ANAT is not enabled, the IP Addressing Mode of the SIP trunk determines what is sent in the SDP body of the SIP Offer, as follows:

- IP Addressing Mode = IPv4 only—The IPv4 address of the MTP is sent in the SDP body.
- IP Addressing Mode = IPv6 only—The IPv6 address of the MTP is sent in the SDP body.
- IP Addressing Mode = IPv4 and IPv6—The cluster-wide IP Addressing Mode Preference for Media (IPv4 or IPv6) is used to determine which MTP address is sent in the SDP body.

**Media Selection for Inbound Early Offer Calls Without ANAT (IPv6 Not Supported)**

IPv6 is not supported.


IPv6 is not supported.
ANAT has not been enabled on the SIP trunk in Figure 7-6, so as with a standard SIP trunk, only a single IP addressing version is exchanged in the SIP Offer and Answer.

**Figure 27: Media Selection on Unified CM SIP Trunks for Inbound Early Offer Calls Without ANAT**

**Call Leg from Trunk MTP to Phone: Standard Unified CM In-Cluster Negotiation**

The MTP is dual-stacked and can match the media addressing type of the phone if it is set to IPv4 only or IPv6 only. If the phone is also dual-stacked, the cluster-wide IP Addressing Mode Preference for Media (IPv4 or IPv6) determines which IP addressing version is used for media.

**Call Leg from Voice Gateway to Trunk MTP: ANAT Not Enabled, and One Media Address Is Received in SDP**

For inbound Early Offer calls where ANAT is not enabled, the IP Addressing Mode of the SIP trunk determines whether the address received in the SDP body of the SIP Offer is accepted or rejected, as follows:

- **IP Addressing Mode = IPv4 only:**
  - If an IPv4 address is received in the SDP body, proceed with the call.
  - If an IPv6 address is received in the SDP body, reject the call.

- **IP Addressing Mode = IPv6 only:**
  - If an IPv6 address is received in the SDP body, proceed with the call.
  - If an IPv4 address is received in the SDP body, reject the call.

**Note**

For these trunk calls, Unified CM does not insert an MTP to resolve a media addressing version mismatch between the two voice devices.
SIP Early Offer Calls with ANAT

Note

This is not supported in CSR 12.0

For the two call scenarios in this section, the SIP trunks use ANAT to exchange and negotiate IPv4 and IPv6 addresses for the media connection between the called and calling endpoints.

Alternative Network Address Types (ANAT)

ANAT is used in the SIP Offer and Answer exchange between dual-stack SIP trunks. ANAT allows devices to send both IPv4 and IPv6 addresses in the SDP body of the SIP Offer, and to return in the SDP body of the SIP Answer, a preferred IP address (IPv4 or IPv6) with which to establish a media connection.

The use of ANAT on a dual-stack SIP trunk is indicated in the header of the SIP Invite. The field Require: sdp-anat is used by Unified CM SIP trunks using Early Offer, and the field Supported: sdp-anat is used by Unified CM SIP trunks using Delayed Offer. The Require: sdp-anat value indicates to the far end of the SIP trunk connection that an ANAT response must be supported. The Supported: sdp-anat value indicates to the far end of the SIP trunk connection that an ANAT response should be supported.

We support ANAT on dual-stack SIP trunks only; that is, on SIP trunks configured with an addressing mode of IPv4 and IPv6.

The receipt of Require: sdp-anat or Supported: sdp-anat does not affect how Unified CM responds to inbound Invites on trunks configured for SIP Early Offer, but it does affect how MTPs are assigned dynamically for inbound calls to Unified CM SIP trunks using Delayed Offer.

Unified CM supports ANAT over dual-stack (IPv4 and IPv6) SIP trunks. If ANAT is enabled, it should be configured on both ends of the SIP trunk. If Require: sdp-anat is sent in the SIP Invite and the receiving SIP trunk does not support ANAT, all calls are rejected. To enable ANAT, check the Enable ANAT check box on the SIP Profile associated with the SIP trunk. ANAT can be used with both Early Offer and Delayed Offer calls.

ANAT should be enabled only on SIP trunks with an IP Addressing Mode setting of IPv4 and IPv6. Enabling ANAT on a single-stack SIP trunk (IPv4 only or IPv6 only) does not really make sense because only one IP address can be offered. Therefore, we do not support ANAT on single-stack (IPv6 only or IPv4 only) SIP trunks.

Media Selection for Outbound Early Offer Calls with ANAT

Note

This is not supported in CSR 12.0

The following figure shows a simplified version the SIP Early Offer and SIP Answer using ANAT on dual-stack SIP trunks.
SIP Early Offer calls involve two call legs: one from the phone to the trunk MTP, and the other from the trunk MTP to the SIP voice gateway. The Cisco IOS MTP is configured to support both IPv4 and IPv6 addresses. ANAT has been enabled on this SIP trunk, so both IPv4 and IPv6 addresses are exchanged in the SIP Offer and Answer.

**Call Leg from Phone to Trunk MTP: Standard Unified CM In-Cluster Negotiation**

The MTP is dual-stacked and can match the media addressing type of the phone if it is set to IPv4-only or IPv6-only. If the phone is also dual-stacked, the cluster-wide IP Addressing Mode Preference for Media (IPv4 or IPv6) determines which IP addressing version is used for media.

**Call Leg from MTP Trunk to Voice Gateway: ANAT Enabled, and Two Media Addresses Sent in SDP (IPv4 and IPv6)**

Unified CM selects the media address preference indicated in the SDP body of the ANAT SIP Offer by using the cluster-wide setting for IP Addressing Mode Preference for Media. The IP Addressing Mode of the trunk must set to IPv4 and IPv6. The trunk's IP Addressing Mode could be set to IPv4-only or IPv6-only, but this would defeat the purpose of ANAT because only one address would be sent. (The trunk's IP Addressing Mode overrides the ANAT setting.)

The called device (voice gateway) selects which addressing version to use for the voice call. The caller's preference does not have to be honored.

**Outbound SIP Early Offer**

The SIP header of the Invite with the outbound SIP Early Offer contains the `Require: sdp-anat` field, indicating that ANAT must be supported by the far-end SIP device. For outbound SIP Offers on Unified CM SIP trunks configured for Early Offer, for all calls the SDP body of the SIP Offer includes the IPv4 address and UDP port number and the IPv6 address and UDP port number of the trunk's statically assigned MTP. The preferred addressing version for Unified CM is also indicated in the SDP body, and the field `a=group:ANAT 2 1` indicates that the second address (the IPv6 address) is preferred by Unified CM. For Early Offer calls, this preference is selected based on the cluster-wide IP Addressing Mode Preference for Media.
Inbound SIP Answer

When the far-end SIP trunk receives an Invite with **Require: sdp-anat**, it must support ANAT and should return an ANAT-based response in its SIP Answer. If ANAT is not supported by the far-end SIP trunk, it should reject the call. In the previous figure, **a=group:ANAT 2** indicates the gateway's choice of its IPv6 address and port number for the voice call. Notice that the gateway's IPv6 address and IPv4 address are both included in the Answer; however, only the IPv6 UDP port number is returned, and the IPv4 UDP port number is set to zero.

Media Selection for Inbound Early Offer Calls With ANAT

---

**Note**

This is **not** supported in CSR 12.0

The following figure shows a simplified version the SIP Early Offer and SIP Answer using ANAT on dual-stack SIP trunks.

SIP Early Offer calls involve two call legs: one from the phone to the trunk MTP, and the other from the trunk MTP to the SIP voice gateway. The Cisco IOS MTP is configured to support both IPv4 and IPv6 addresses. ANAT has been enabled on this SIP trunk, so both IPv4 and IPv6 addresses will be exchanged in the SIP Offer and Answer.

---

**Figure 29: Media Selection on Unified CM SIP Trunks for Inbound Early Offer Calls with ANAT**

---

Call Leg from Trunk MTP to Phone: Standard Unified CM In-Cluster Negotiation

The MTP is dual-stacked and can match the media addressing version of the phone if it is set to IPv4-only or IPv6-only. If the phone is also dual stacked, the cluster-wide IP Addressing Mode Preference for Media (IPv4 or IPv6) is used to select which IP addressing version is used for media.
Call Leg from Voice Gateway to Trunk MTP: ANAT Enabled, and IPv4 and IPv6 Media Addresses Received in SDP

Unified CM does not honor the indicated address preference in the SDP body of the received SIP Offer. For dual-stack Unified CM SIP trunks (IP Addressing Mode = IPv4 and IPv6), Unified CM selects the addressing version for the voice call based on the setting of the cluster-wide IP Addressing Mode Preference for Media.

Inbound SIP Early Offer

The SIP header of the Invite with the outbound SIP Early Offer contains the Require: sdp-anat field, indicating that ANAT must be supported by Unified CM. The SDP body of the SIP Offer includes the IPv4 address and UDP port number and the IPv6 address and UDP port number of the calling device. The preferred addressing version of the calling device is also indicated in the SDP body, and the field a=group:ANAT2 indicates that the second address (the IPv6 address) is preferred.

Outbound SIP Answer

When the Unified CM SIP Early Offer trunk receives an Invite with Require: sdp-anat, it must support ANAT and should return an ANAT-based response in its SIP Answer. If ANAT is not supported by the Unified CM SIP trunk, it will reject the call. For Unified CM trunks configured for Early Offer, Unified CM returns the IPv4 and IPv6 addresses of the trunk MTP in its SIP Answers. In the previous figure, a=group:ANAT2 indicates Unified CM’s choice for the IPv6 address and port number of the MTP for the voice call. Notice that the MTP’s IPv6 address and IPv4 address are both included in the Answer; however, only the IPv6 UDP port number is returned, and the IPv4 UDP port number is set to zero.

---

**Note**

Unified CM selects the addressing version for the voice call based on the setting of the cluster-wide IP Addressing Mode Preference for Media. The incoming preference is not honored by Unified CM.

---

**SIP Trunks Using Delayed Offer**

With Delayed Offer, SIP trunks do not use a statically assigned MTP, and typically only one call leg is created between the calling phone and called phone or device. From the perspective of Unified CM, this makes the selection of which IP addressing version to use a little more involved because in this case both the trunk's settings and the phone's settings must be taken into account.

**Media Selection for Outbound Delayed Offer Calls Over Unified CM SIP Trunks Without ANAT**

As shown in the following figure, SIP Delayed Offer calls typically involve a single call leg from the phone to the SIP voice gateway. ANAT has not been enabled on this SIP trunk, so as with a standard SIP trunk, only a single IP addressing version is exchanged in the SIP Offer and Answer.
For outbound Delayed Offer calls, the IP Addressing Mode settings of both the trunk and the phone influence the call setup in the following ways:

- The IP Addressing Mode setting of the trunk determines whether the received SIP Offer is accepted or rejected.
- The IP Addressing Mode setting of the phone determines which address (phone or MTP) is returned in the SIP Answer from Unified CM.

In this scenario, Unified CM can dynamically insert an MTP, if needed, into the call to convert the IP addressing version of the voice media stream between the calling and called devices. As mentioned previously, dynamically inserted MTPs support the pass-through codec, allowing video calls and encrypted calls to be established.

**IP Addressing Mode of the Trunk**

- IP Addressing Mode = IPv4 only:
  - If an IPv4 address is received in the SDP body, proceed with the call.
  - If an IPv6 address is received in the SDP body, reject the call.

- IP Addressing Mode = IPv6 only:
  - If an IPv6 address is received in the SDP body, proceed with the call.
  - If an IPv4 address is received in the SDP body, reject the call.

**Note**

For trunk call signaling, Unified CM does not insert an MTP to resolve a media addressing version mismatch.

- IP Addressing Mode = IPv4 and IPv6 (Recommended configuration):
  - If an IPv4 address is received in the SDP body, proceed with the call.
• If an IPv6 address is received in the SDP body, proceed with the call.

For SIP trunks using Delayed Offer and not using ANAT, the recommended trunk IP Addressing Mode setting is IPv4 and IPv6 because both IPv6 calls and IPv4 calls are accepted by the trunk.

**IP Addressing Mode of the Phone**

- **IP Addressing Mode = IPv4 only:**
  - If an IPv4 address is received in the SDP body, proceed with the call and return the IPv4 address of the phone in the SDP body of the SIP answer.
  - If an IPv6 address is received in the SDP body, dynamically insert an MTP into the media path to convert IP addressing versions, then proceed with the call. Return the IPv6 address of the MTP in the SDP body of the SIP answer.

- **IP Addressing Mode = IPv6 only:**
  - If an IPv6 address is received in the SDP body, proceed with the call and return the IPv6 address of the phone in the SDP body of the SIP answer.
  - If an IPv4 address is received in the SDP body, dynamically insert an MTP into the media path to convert IP addressing versions, then proceed with the call. Return the IPv4 address of the MTP in the SDP body of the SIP answer.

- **IP Addressing Mode = IPv4 and IPv6:**
  - If an IPv4 address is received in the SDP body, proceed with the call and return the IPv4 address of the phone in the SDP body of the SIP answer.
  - If an IPv6 address is received in the SDP body, proceed with the call and return the IPv6 address of the phone in the SDP body of the SIP answer.

**When an MTP Is Required, Will the MTP of the Phone or the Trunk Be Used?**

The cluster-wide IP Addressing Mode Preference for Media determines whether the MTP of the phone or of the trunk is used to convert the voice media stream between IPv4 and IPv6. This preference is used to select an MTP so that the longest Real-Time Transport Protocol (RTP) call leg in the cluster matches the cluster-wide preference.

**Deployment Considerations for Delayed Offer Calls over Trunks without ANAT**

If a call from an IPv4-only phone receives a SIP Offer that contains an IPv6 address, or if a call from an IPv6-only phone receives a SIP Offer that contains an IPv4 address, Unified CM dynamically inserts an MTP to convert between IPv4 and IPv6. In deployments with large numbers of IPv4-only phones, any SIP trunk call to or from an IPv6-only device requires an MTP for conversion between IPv4 and IPv6. Therefore, we recommend that you provide MTP resources for IPv4-only and IPv6-only devices in the Unified CM cluster.
Media Selection for Inbound Delayed Offer Calls Over Unified CM SIP Trunks Without ANAT

As shown in the following figure, SIP Delayed Offer calls typically involve a single call leg from the phone to the SIP voice gateway. ANAT has not been enabled on this SIP trunk, so as with a standard SIP trunk, only a single IP addressing version is exchanged in the SIP Offer and Answer.

**Figure 31: Media Selection on Unified CM SIP Trunks for Inbound Delayed Offer Calls Without ANAT**

For inbound Delayed Offer calls, the combined settings of the IP Addressing Mode of both the trunk and the phone determine which IP addressing version and which device's IP address is sent in the SDP body of the SIP Offer.

For inbound Delayed Offer calls, if a mismatch exists between the IP addressing modes of the phone and the trunk, Unified CM can dynamically insert an MTP into the call path to convert the IP addressing version of the voice media stream from the IP phone, so that it matches that configured on the trunk. In this case, the address of the MTP is sent in the SDP body of Unified CM's SIP Offer.

For SIP trunks using Delayed Offer and not using ANAT, the recommended IP Addressing Mode setting for the trunk is **IPv4 and IPv6**. With this setting, Unified CM does not need to insert MTPs for inbound SIP Delayed Offer calls.

**When an MTP Is Required, Will the MTP of the Phone or the Trunk Be Used?**

The cluster-wide IP Addressing Mode Preference for Media determines whether the MTP of the phone or of the trunk is used to convert the voice media stream between IPv4 and IPv6. See the following table for details. This preference is used to select an MTP so that the longest Real-Time Transport Protocol (RTP) call leg in the cluster matches the cluster-wide preference.

As mentioned previously, dynamically inserted MTPs do support the pass-through codec, allowing video calls and encrypted calls to be established.
Table 13: IP Addressing Mode Preference for Media

<table>
<thead>
<tr>
<th>IP Addressing Mode of Phone</th>
<th>IP Addressing Mode of Trunk</th>
<th>Address Sent in SIP Offer by Unified CM</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4 Only</td>
<td>IPv4 Only</td>
<td>IPv4 address of phone</td>
</tr>
<tr>
<td>IPv4 Only</td>
<td>IPv4 and IPv6</td>
<td>IPv4 address of phone</td>
</tr>
<tr>
<td>IPv6 Only</td>
<td>IPv4 Only</td>
<td>IPv6 address of phone</td>
</tr>
<tr>
<td>IPv6 Only</td>
<td>IPv4 and IPv6</td>
<td>IPv6 address of phone</td>
</tr>
<tr>
<td>IPv4 Only</td>
<td>IPv6 Only</td>
<td>Insert an MTP and use its IPv6 address</td>
</tr>
<tr>
<td>IPv6 Only</td>
<td>IPv4 Only</td>
<td>Insert an MTP and use its IPv4 address</td>
</tr>
<tr>
<td>IPv4 and IPv6</td>
<td>IPv4 Only</td>
<td>IPv4 address of phone</td>
</tr>
<tr>
<td>IPv4 and IPv6</td>
<td>IPv6 Only</td>
<td>IPv6 address of phone</td>
</tr>
<tr>
<td>IPv4 and IPv6</td>
<td>IPv4 and IPv6 Only</td>
<td>IPv4 or IPv6 address of phone&lt;sup&gt;1&lt;/sup&gt;</td>
</tr>
</tbody>
</table>

<sup>1</sup> The cluster-wide IP Addressing Mode Preference for Media determines which phone address (IPv4 or IPv6) Unified CM sends in the SDP body of the SIP Offer.

Media Selection for Delayed Offer Calls Over Unified CM SIP Trunks With ANAT

In the following call scenarios, the SIP trunks use ANAT to exchange IPv4 and IPv6 addresses for the media connection between the called and calling endpoints:

- Outbound Delayed Offer calls with ANAT.
- Inbound Delayed Offer calls with ANAT, where **Supported: sdp-anat** is received.
- Inbound Delayed Offer calls with ANAT, where **Require: sdp-anat** is received.

**Alternative Network Address Types (ANAT)**

ANAT is used in the SIP Offer and Answer exchange between dual-stack SIP trunks. ANAT allows SIP devices to send both IPv4 and IPv6 addresses in the SDP body of the SIP Offer, and to return in the SDP body of the SIP Answer, the preferred IP address (IPv4 or IPv6) with which to establish a media connection.

The use of ANAT on a SIP trunk is indicated in the header of the SIP Invite. The field **Require: sdp-anat** is used by Unified CM SIP trunks using Early Offer, and the field **Supported: sdp-anat** is used by Unified CM SIP trunks using Delayed Offer. The **Require: sdp-anat** value indicates to the far end of the SIP trunk connection that an ANAT response must be supported. The **Supported: sdp-anat** value indicates to the far end of the SIP trunk connection that an ANAT response should be supported.
For inbound calls to Unified CM SIP trunks using Delayed Offer, the receipt of these require or supported sdp-anat values by Unified CM has the following effects on how MTPs are assigned dynamically:

- If Unified CM receives an Invite with **Require: sdp-anat**, it returns two IP addresses in the SDP body of its ANAT SIP Offer (and therefore inserts an MTP for calls to IPv4-only and IPv6-only devices).

- If Unified CM receives an Invite with **Supported: sdp-anat**, it returns the IP addresses supported by the called device in the SDP body of its SIP Offer. In the case of an IP addressing version mismatch between the calling and called device for calls between Unified CM clusters, the calling Unified CM cluster inserts an MTP for conversions between IPv4 and IPv6.

- MTPs are not needed for calls to ANAT-enabled dual-stack Unified CM SIP trunks where **Supported: sdp-anat** is received; whereas when **Require: sdp-anat** is received by Unified CM, MTPs are needed for single-stack (IPv4-only or IPv6-only) endpoints.

Unified CM supports ANAT over dual-stack (IPv4 and IPv6) SIP trunks. If ANAT is enabled, it should be configured on both ends of the SIP trunk. (If **Require: sdp-anat** is sent in the SIP Invite and the receiving SIP trunk does not support ANAT, all calls are rejected.) To enable ANAT, check the **Enable ANAT** check box on the SIP Profile associated with the SIP trunk. ANAT can be used with both Early Offer and Delayed Offer calls.

ANAT should be enabled only on SIP trunks with an IP Addressing Mode setting of **IPv4 and IPv6**. Enabling ANAT on a single-stack SIP trunk (IPv4 only or IPv6 only) does not really make sense because only one IP address can be offered.

### Media Selection for Outbound Delayed Offer Calls with ANAT

The following figure shows a simplified version of the SIP Delayed Offer and SIP Answer using ANAT on dual-stack SIP trunks.

SIP Delayed Offer calls typically involve a single call leg from the phone to SIP voice gateway. For outbound SIP Delayed Offer calls, Unified CM sends **Supported: sdp-anat** in its SIP Invite.

*Figure 32: Media Selection on Unified CM SIP Trunks for Outbound Delayed Offer Calls with ANAT*
Outbound SIP Invite

The SIP header of the outbound Delayed Offer SIP Invite contains Supported: sdp-anat, indicating to the far-end device that ANAT is supported by this Unified CM trunk and should be supported by the far-end trunk. If ANAT is not supported by the far-end trunk, the call can still proceed, and only a single IP address is returned in the (non-ANAT) SIP Offer. In this case, Unified CM selects a media address (and inserts MTPs if required), as described in Media Selection for Outbound Delayed Offer Calls Over Unified CM SIP Trunks Without ANAT, on page 78.

Inbound SIP Delayed Offer

The SDP body of the inbound SIP Offer includes the IPv4 address and UDP port number as well as the IPv6 address and UDP port number of the voice gateway. The preferred addressing version of the gateway is also indicated in the SDP body, and a=group:ANAT 2 1 indicates that the second address (the IPv6 address) is preferred by the gateway. For Cisco IOS gateways, the ANAT IP addressing version preference is configured at the voice service voip level using the protocol mode dual-stack preference CLI command.

Outbound SIP Answer

With ANAT supported but not required, the SIP Answer from Unified CM does not have to contain both an IPv4 and an IPv6 address. If the calling device supports IPv4 Only or IPv6 Only, then only a single IP address is sent in the SDP body of the outbound SIP Answer. For the call shown in the previous figure, both the calling phone and trunk support both IPv4 and IPv6, in which case both addresses of the phone are sent in the SIP Answer. The a=group:ANAT 2 indicates Unified CM's choice of the phone's IPv6 address and port number for the voice call. In this example, the phone's IPv6 address and IPv4 address are both included in the SIP Answer; however, only the IPv6 UDP port number is returned, and the IPv4 UDP port number is set to zero.

Note

Unified CM does not have to honor the IP addressing version preference received in the SIP Offer. The media addressing version preference sent by Unified CM in the SDP Answer is set by the cluster-wide IP Addressing Mode Preference for Media.

Table 14: Addresses Sent in the SIP Answer from a Dual-Stack ANAT-Enabled Unified CM SIP Trunk

<table>
<thead>
<tr>
<th>IP Addressing Mode of Phone</th>
<th>IP Addressing Mode of Trunk</th>
<th>Address Sent in SIP Answer by Unified CM</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4</td>
<td>IPv4 and IPv6</td>
<td>IPv4 address of the phone</td>
</tr>
<tr>
<td>IPv6</td>
<td>IPv4 and IPv6</td>
<td>IPv6 address of the phone</td>
</tr>
<tr>
<td>IPv4 and IPv6</td>
<td>IPv4 and IPv6</td>
<td>IPv4 and IPv6 addresses of the phone²</td>
</tr>
</tbody>
</table>

² The media addressing version preference sent in the SDP Answer is set by the cluster-wide IP Addressing Mode Preference for Media.

When only one valid IP address and UDP port number is available to be returned by Unified CM in the SIP Answer, a second invalid address (typically the IPv4 or IPv6 address received in the SIP Offer) is returned in the SIP Answer, with its UDP port number set to 0.
Inbound Delayed Offer Calls with ANAT

Based on the far-end trunk configuration, inbound SIP Invites to Unified CM from a trunk using Delayed Offer and ANAT could contain either **Require: sdp-anat** or **Supported: sdp-anat** in the SIP header. Dual-stack Unified CM SIP trunks respond as follows to inbound calls with each of these settings:

- With **Require: sdp-anat**, Unified CM always sends a valid IPv4 address and a valid IPv6 address in the SIP Offer.
- With **Supported: sdp-anat**, Unified CM sends the IP addresses supported by the called device.

For inbound calls to ANAT-enabled dual-stack Unified CM SIP trunks where **Supported: sdp-anat** is received in the SIP Invite, Unified CM does not have to use MTPs; whereas when **Require: sdp-anat** is received by Unified CM, MTPs must be used for single-stack (IPv4-only or IPv6-only) endpoints.

**Note**

Unified CM trunks always send **Supported: sdp-anat** in Delayed Offer SIP Invites. The default setting for Cisco IOS gateways is to send **Require: sdp-anat** Early Offer calls.

Inbound Delayed Offer Calls with ANAT and Supported: sdp-anat

The following figure shows a simplified version of the SIP Offer and SIP Answer using ANAT, where the calling trunk sends **Supported: sdp-anat** in its SIP Invite. As illustrated, SIP Delayed Offer calls typically involve a single call leg from the phone to the SIP voice gateway.

**Figure 33: Media Selection on Unified CM SIP Trunks for Inbound Delayed Offer Calls with ANAT and Supported: sdp-anat**

Inbound SIP Invite

The SIP header of the inbound Delayed Offer SIP Invite contains **sdp-anat** in the Supported field, indicating to Unified CM that an ANAT response should be supported by this trunk. For Cisco IOS gateways, you can
configure the ANAT IP addressing version preference at the `voice service voip` level by using the following CLI command.

```plaintext
protocol mode dual-stack preference
```

### Outbound SIP Offer

With ANAT supported but not required, Unified CM's outbound SIP Offer does not have to contain both an IPv4 address and an IPv6 address. If the called device supports IPv4 Only or IPv6 Only, then only a single IP address is sent in the SDP body of the SIP Offer. For the call shown in the previous figure, both the called phone and the trunk support both IPv4 and IPv6, in which case the SDP body of the SIP Delayed Offer includes the IPv4 address and UDP port number as well as the IPv6 address and UDP port number of the called IP phone. The preferred addressing version of Unified CM is also indicated in the SDP body, and `a=group:ANAT 2 1` indicates that the second address (the IPv6 address) is preferred by Unified CM. For outbound Delayed Offer calls, this preference is selected based on the cluster-wide IP Addressing Mode Preference for Media.

### Inbound SIP Answer

If Unified CM sends a single address in its SIP Offer, the calling trunk should respond as if it is a Delayed Offer call without ANAT enabled. For the call shown in the previous figure, both the called phone and the trunk support both IPv4 and IPv6. In the received SIP Answer, `a=group:ANAT 2` indicates the gateway's choice of its IPv6 address and port number for the voice call. Both the gateway's IPv6 address and its IPv4 address are included in the SIP Answer; however, only the IPv6 UDP port number is returned, and the IPv4 UDP port number is set to zero.

---

**Note**

The called device does not have to honor the IP addressing version preference of the calling device.

If only one IP address is available to be sent in the SIP Offer, then only this single IP address is sent, and accordingly only one address (of the same IP addressing version) is expected in the SIP Answer.

### Table 15: Addresses Sent in the SIP Offer from a Dual-Stack ANAT-Enabled Unified CM SIP Trunk

<table>
<thead>
<tr>
<th>IP Addressing Mode of Phone</th>
<th>IP Addressing Mode of Trunk</th>
<th>Address Sent in SIP Offer from Unified CM</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4</td>
<td>IPv4 and IPv6</td>
<td>IPv4 address of phone</td>
</tr>
<tr>
<td>IPv6</td>
<td>IPv4 and IPv6</td>
<td>IPv6 address of phone</td>
</tr>
<tr>
<td>IPv4 and IPv6</td>
<td>IPv4 and IPv6</td>
<td>IPv4 and IPv6 addresses of phone</td>
</tr>
</tbody>
</table>

---

### Inbound Delayed Offer Calls with ANAT and Require: sdp-anat

The following figure shows a simplified version of the SIP Offer and SIP Answer using ANAT, where the calling device sends `Require: sdp-anat` in its SIP Invite. As illustrated, SIP Delayed Offer calls typically involve a single call leg from the phone to the SIP voice gateway.
Inbound SIP Invite

The SIP header of the inbound Delayed Offer SIP Invite contains sdp-anat in the Require field, indicating that ANAT responses must be supported by this Unified CM trunk. For Cisco IOS gateways, you can configure the ANAT IP addressing version preference at the voice service voip level by using the following CLI command.

```
  protocol mode dual-stack preference
```

Outbound SIP Offer

With ANAT required, Unified CM's SIP Offer must contain both an IPv4 and an IPv6 address. If the called device supports an addressing mode of IPv4 Only or IPv6 Only, then Unified CM dynamically inserts an MTP and sends its IPv4 address and its IPv6 address in the SDP body of the SIP Offer. For the call shown in the previous figure both the called phone and trunk support both IPv4 and IPv6, in which case the SDP body of the SIP Delayed Offer includes the IPv4 address and UDP port number as well as the IPv6 address and UDP port number of the called IP phone. Unified CM's preferred addressing version is also indicated in the SDP body, and `a=group:ANAT21` indicates that the second address (the IPv6 address) is preferred by Unified CM. For Outbound Delayed Offer calls, the cluster-wide IP Addressing Mode Preference for Media determines this preference.

Inbound SIP Answer

When ANAT is required by the calling trunk, it sends an ANAT-based response in its SIP Answer. In the received SIP Answer, `a=group:ANAT2` indicates the gateway's choice of its IPv6 address and port number for the voice call. Both the gateway's IPv6 address and its IPv4 address are included in the SIP Answer; however, only the IPv6 UDP port number is returned, and the IPv4 UDP port number is set to zero.

---

Note

The called device does not have to honor the IP addressing version preference of the calling device.

For inbound Delayed Offer calls with Require: sdp-anat in the received Invite, the IP Addressing Mode of the trunk is set to IPv4 and IPv6. If a mismatch exists between the phone's and the trunk's IP Addressing...
Modes, Unified CM dynamically inserts an MTP into the call path and sends the MTP's IPv4 and IPv6 addresses in the SDP body of SIP Offer from Unified CM.

**When an MTP Is Required, Will the MTP of the Phone or the Trunk Be Used?**

The cluster-wide IP Addressing Mode Preference for Media determines whether the MTP of the phone or of the trunk is used to convert the voice media stream between IPv4 and IPv6. This preference is used to select an MTP so that the longest Real-Time Transport Protocol (RTP) call leg in the cluster matches the cluster-wide preference.

Dynamically inserted MTPs do support the pass-through codec, allowing video calls and encrypted calls to be established.

**Table 16: Addresses Sent in the SIP Offer from a Dual-Stack ANAT-Enabled Unified CM SIP Trunk**

<table>
<thead>
<tr>
<th>IP Addressing Mode of Phone</th>
<th>IP Addressing Mode of Trunk</th>
<th>Address sent in SIP Offer from Unified CM</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4</td>
<td>IPv4 and IPv6</td>
<td>Insert MTP, and send IPv4 and IPv6 addresses of MTP.</td>
</tr>
<tr>
<td>IPv6</td>
<td>IPv4 and IPv6</td>
<td>Insert MTP, and send IPv4 and IPv6 addresses of MTP.</td>
</tr>
<tr>
<td>IPv4 and IPv6</td>
<td>IPv4 and IPv6</td>
<td>IPv4 and IPv6 addresses of phone</td>
</tr>
</tbody>
</table>
CHAPTER 8

Media Resources and Music on Hold

• Media Resources and Music on Hold Overview, on page 89
• Media Termination Point (MTP), on page 89
• IPv6 and Other Media Resources, on page 92

Media Resources and Music on Hold Overview

A media resource is a software-based or hardware-based entity that performs media processing functions on the data streams to which it is connected. Media processing functions include mixing multiple streams to create one output stream (conferencing), passing the stream from one connection to another (media termination point), converting the data stream from one compression type to another (transcoding), echo cancellation, signaling, termination of a voice stream from a TDM circuit (coding and decoding), packetization of a stream, streaming audio (Annunciator and Music on Hold), and so forth.

This chapter focuses on new media termination point (MTP) functionality introduced to support IPv6 Collaboration deployments: namely, the capability of Cisco IOS MTPs to convert a voice media stream from IPv4 to IPv6 and conversely. Other media resources such as conferencing and transcoding are also discussed in context with this new MTP functionality. For all other media resource and Music on Hold (MoH) design guidance, refer to the Cisco Collaboration System Solution Reference Network Design (SRND), available at http://www.cisco.com/go/ucsrnd.

Media Termination Point (MTP)

The following Cisco Integrated Services Router (ISR) MTPs support media conversion between IPv4 and IPv6 for devices with mismatched media IP address versions:

• Cisco IOS hardware MTPs—Digital signal processors (DSPs) on the Cisco ISR Motherboard and NM-HDV2 with PVDM2 DSPs
• Cisco IOS software MTPs

Cisco IOS Release IOS XE Everest 16.6.1 and above supports these MTPs.
Address Conversion Between IPv4 and IPv6

When a mismatch exists between the IP addressing versions supported by two devices, Unified CM dynamically inserts an MTP resource to convert the voice media stream from IPv4 to IPv6 and conversely. Dynamically inserted MTPs support the pass-through codec, which allows the MTP to support not only voice calls but also video calls and encrypted calls. The pass-through codec should be configured on all dynamically inserted MTPs. To enable the use of the pass-through codec, configure the MTP with both a standard codec and the pass-through codec.

Unified CM trunks can also be configured with a statically assigned MTP (MTP Required check box checked). The trunk's statically defined MTP does not support the pass-through codec and supports only a single configured codec (G.711 or G.729), which limits all calls that use this trunk to either G.711 or G.729 voice calls and T.38 Fax calls only. This statically assigned MTP also has the capability to convert the voice media stream from IPv4 to IPv6 and conversely.

To be dynamically or statically inserted into a call path, the Cisco IOS MTPs must be associated with the media resource group (MRG) for each device (phone or trunk).

The following Cisco IOS configuration is an example of a software MTP. The `sccp local GigabitEthernet0/0` command associates the IPv4 and IPv6 addresses on this interface with the MTP for both SCCP signaling and media addresses.

```
interface GigabitEthernet0/0
ip address 192.168.1.5 255.255.255.0
! MTP's IPv4 address
ipv6 address 2001:0db8:101:1:1::5/64
! MTP's IPv6 address
!
sccp local GigabitEthernet0/0
sccp ccm 192.168.0.15 identifier 1 version 7.0
! Unified CM's IPv4 address
sccp ccm 2001:0db8:101:1::15 identifier 2 version 7.0
! Unified CM's IPv6 address
sccp
!
sccp ccm group 1
associate ccm 1 priority 1
associate ccm 2 priority 2
associate profile 1 register MTP-1
!
dspfarm profile 1 mtp
codec g711ulaw
codec pass-through
maximum sessions software 100
associate application SCCP
!
```

The following figure shows when an MTP is inserted between two devices to convert from IPv4 to IPv6, and conversely. However, both devices can have MTP resources available in their media resource groups, and Unified CM must decide which MTP to use. Unified CM uses the cluster-wide setting of IP Addressing Mode Preference for Media to determine which MTP to use for conversions between IPv4 and IPv6.
If the cluster-wide IP Addressing Mode Preference for Media is set to IPv6, Unified CM chooses the MTP associated with the IPv4 device.

Conversely, if the cluster-wide IP Addressing Mode Preference for Media is set to IPv4, Unified CM chooses the MTP associated with the IPv6 device.
By choosing the device whose addressing mode does not match the cluster-wide IP Addressing Mode Preference for Media, Unified CM selects the cluster-wide media preference value that matches the longest call leg between the two devices in the cluster.

**Note**

If the preferred device's MTP is not available, the other device's MTP is used as a last resort. If no MTPs are available, the call fails.

Transcoder DSP resources can also be used as hardware MTPs. If both transcoding resources and software MTPs exist in the same media resource group, Unified CM uses these media resources in a round-robin fashion for conversions between IPv4 and IPv6. To prioritize transcoding DSP resources for transcoding purposes only, place the software MTP and hardware MTPs in a separate media resource group (MRG) and give this MRG precedence (a higher order) over the transcoder MRG in the media resource group list (MRGL).

The number of MTPs required is based on the traffic that requires media header addressing conversation from IPv4 to IPv6. In the worst case, the number of MTPs required is the same as the number of IPv6-only devices that are in service. The MTPs should be located in a site where IPv4-only phones are deployed. For IPv6-only sites, the MTPs should be located where servers are deployed, for example, in a data center. MTPs should be located where IPv4 and IPv6 addresses are available. Quicker transition to IPv6-only devices is recommended to phase out MTPs from a network.

**IPv6 and Other Media Resources**

The following media resources do not support IPv6 for voice. If these resources are invoked, an MTP resource is required to convert the voice stream between IPv6 and IPv4, as shown in the following figure.

- Video conferencing
- Video Transcoding
- IPv6 Music on Hold (MoH)
Voice conferencing resources and hardware MTP resources can reside on the same DSP. Similarly, voice transcoding resources and hardware MTP resources can reside on the same DSP.

IPv6-only devices do not support multicast music on hold.

**Cisco IOS RSVP Agent and IPv6**

The Cisco IOS Resource Reservation Protocol (RSVP) agent does not support IPv6, and RSVPv4 cannot be used within the cluster for call admission control. For SIP trunks and intercluster trunks, locations-based call admission control must be used.

**IPv4 to IPv6 Conversion When Multiple MTPs Exist Within a Media Resource Group (MRG)**

Unified CM server-based MTPs do not support the pass-through codec. If Cisco IOS MTPs (which support the pass-through codec) and Unified CM MTPs (which do not support the pass-through codec) are listed in the same media resource group, Unified CM requests an MTP with pass-through codec support for conversions between IPv4 and IPv6.

If an MTP is statically assigned to the SIP trunk (Early Offer), then conversions between IPv4 and IPv6 can occur only for the codec specified on the MTP (G.711 or G.729).
Call Processing and Call Admission Control Overview

This chapter discusses aspects of call processing and call admission control that apply specifically to IPv6.

Call Processing

This section describes a few changes to call processing operation for IPv6, along with some IPv6 configuration information. For information on designing scalable and resilient call processing systems with Cisco Unified Communications Manager (Unified CM), refer to the Cisco Collaboration System Solution Reference Network Design (SRND), available at http://www.cisco.com/go/ucsrnd.

Enable Call Processing for IPv6

To enable call processing for IPv6, you must first enable IPv6 throughout the Cisco Unified Communications Manager (Unified CM) cluster, as outlined in the following steps:

1. Configure IPv6 on each server in the Unified CM cluster, either through the server operating system (OS) command line interface (CLI) or through the Cisco Unified Operating System Administration graphical user interface (GUI).
2. Configure IPv6 in Cisco Unified CM Administration.

Configure IPv6 on Each Server in Cluster Using CLI

Before you enable IPv6 in Cisco Unified CM Administration, you must configure IPv6 on each server in the cluster by using the following server operating system (OS) CLI commands:
**Procedure**

**Step 1**
Enable IPv6 by using the `set network ipv6 service enable` command.

**Step 2**
Set a static IPv6 address for your server by using the `set network ipv6 static_address <addr> <mask>` command. The DHCPv6 client is also supported, but its use is not recommended.

**Step 3**
To view the platform's IPv6 address settings, use the `show network ipv6 settings` command. Example output from this command is as follows:

```
IPv6 : enabled
DHCPv6 : disabled
IPv6 addresses:
Address:2001:db8:c18:1:21c:c4ff:feef:ca0 Mask:64
Scope:Global Duplicate:no
Address:fe80::21c:c4ff:feef:ca0 Mask:64
Scope:Link
```

**Configure Unified CM Server IPv6 Address Using GUI**

You can configure the IPv6 address of the server platform by using the Cisco Unified Operating System Administration GUI.

**Procedure**

To set the address, select **Settings > IP > Ethernet IPv6**.

The following figure shows how to configure the IPv6 address of the server platform by using the Cisco Unified Operating System Administration GUI.
Define Unified CM Server IPv6 Addresses

After you configure the server platform IPv6 address, define the IPv6 address for each Unified CM server by using Cisco Unified CM Administration. Select System > Server, and enter the IPv6 address in the IPv6 Name field. This IPv6 address allows IP phones to retrieve the IPv6 address of this Unified CM from the configuration file downloaded from the TFTP server.
Cluster-Wide IPv6 Configuration

You can configure the following cluster-wide IPv6 settings for each Unified CM server through the Enterprise Parameters page for IPv6 and IPv6 for Phones in Unified CM Administration:

- Enable IPv6 (Set to True)
- IP Addressing Mode Preference for Media (Set to IPv6)
- IP Addressing Mode Preference for Signaling (Set to IPv6)
- Allow Auto-Configuration for Phones (Set to On)
Enable IPv6

Set this parameter to True to enable IPv6. The default setting is False.

IP Addressing Mode Preference for Media

This parameter has two setting options:

- IPv4 (Default)
- IPv6 (Set to IPv6)

This cluster-wide IP Addressing Mode Preference for Media is different than the device-level IP addressing mode, and it serves two purposes:

- The cluster-wide Addressing Mode Preference for Media is used to select which IP addressing version to use for media when a call is made between two dual-stack devices.
- The cluster-wide Addressing Mode Preference for Media is also used when there is a mismatch in supported IP addressing versions between two devices. If an IPv6-only device calls an IPv4-only device, an MTP must be inserted into the media path to convert between IPv4 and IPv6. Typically both devices will have MTP media resources available to them in their media resource group (MRG). The cluster-wide Addressing Mode Preference for Media determines which device's MTP is used to convert between IPv4 and IPv6 for the call.

MTP resource allocation is discussed in detail in Media Resources and Music on Hold Overview, on page 89.

IP Addressing Mode Preference for Signaling

The cluster-wide IP Addressing Mode Preference for Signaling setting is used by devices whose IP Addressing Mode Preference for Signaling is set to Use System Default. The cluster-wide IP Addressing Mode Preference for Signaling has two setting options:

- IPv4 (Default)
• IPv6 (Set to IPv6)

**Allow Auto-Configuration for Phones**

The cluster-wide setting of Allow Auto-Configuration for Phones is used by phones whose Allow Auto-Configuration for Phones parameter is set to *Default*. Allow Auto-Configuration for Phones has two settings:

• On (Default)
• Off

**Unified CM Server Hardware Platforms**

All standard Unified CM hardware platforms can support IPv6. Unified CM clusters use various types of servers, depending on the scale, performance, and redundancy required. They range from non-redundant, single-processor servers to highly redundant, multi-processor units. For a list of the general types of servers you can use in a Unified CM cluster, along with their main characteristics, refer to the *Cisco Collaboration System Solution Reference Network Design (SRND)*, available at [http://www.cisco.com/go/ucsrnd](http://www.cisco.com/go/ucsrnd).

**NIC Teaming for Network Fault Tolerance**

NIC teaming for Network Fault Tolerance with Unified CM is supported for IPv6 on Hewlett-Packard and IBM server platforms with dual Ethernet network interface cards (NICs). This feature allows a server to be connected to the Ethernet through two NICs and, hence, two cables. NIC teaming prevents network downtime by transferring the workload from the failed port to the working port. NIC teaming cannot be used for load balancing or increasing the interface speed.

**Intra-Cluster Communications**

There are two primary types of intra-cluster communications, database replication and Intra-Cluster Communication Signaling (ICCS), both of which support IPv4-only.

**TFTP Server**

Within any Unified CM system, endpoints such as IP phones rely on a TFTP process to acquire configuration files, software images, and other endpoint-specific information. The Cisco TFTP service is a file serving system that can run on one or more Unified CM servers. It builds configuration files and serves firmware files, ringer files, device configuration files, and so forth, to endpoints.

When IPv6 is enabled in the Unified CM cluster, the TFTP server inherits its IPv6 server address from the configured server address. This allows the TFTP server to serve files to devices using IPv6 signaling.

**Unified CM 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.
Unified CM AXL/SOAP

Unified CM's Administrative XML (AXL) Simple Object Access Protocol (SOAP) interface is IPv6-aware. The AXL/SOAP interface communicates with IPv4 addresses, but it can receive and understand IPv6 addresses embedded in application protocol data units (PDUs).

SNMP

Simple Network Management Protocol (SNMP) for Unified CM includes:
- SNMPv6 MIB support.
- Ability to accept SNMP requests from v6-only hosts.
- Ability to configure v6-only SNMP Notification Destination.
- IPv6 support for SNMP V1/V2C/V3 protocols.

Cisco Collaboration Applications

Cisco Collaboration applications servers that are documented in this document are dual-stack, but Cisco Prime Collaboration is IPv6-aware. All the third-party applications remain in IPv4-only and are IPv6 aware where applicable.

Unified CM Platform Capacity Planning

IPv6 addresses require more Unified CM server memory when compared with IPv4 addresses. Therefore, in a Unified CM deployment with many IPv6 devices, the busy hour call completion (BHCC) capacity is approximately 3% to 5% less than the capacity of IPv4-only deployments.

Interoperability of Unified CM and Unified CM Express

Cisco Unified Communications Manager Express (Unified CME) supports IPv4-only. If you are deploying Unified CME with Unified CM, the interface is IPv4-only. Follow the design guidance in the Cisco Collaboration System Solution Reference Network Design (SRND), available at http://www.cisco.com/go/ucsrnd.

Call Admission Control (CAC)

IPv6-enabled Unified CM supports single-site deployments, multi-site WAN deployments with distributed call processing, and multi site deployments with centralized call processing. Call admission control is required where calls are made over a WAN between remote sites on the same cluster or between Unified CM clusters.
Call Admission Control with Unified Communications IPv6 Deployments

Collaboration IPv6 deployments with Unified CM support locations-based topology-unaware call admission control only for calls between remote sites in the same cluster and over intercluster trunks. Topology-unaware call admission control requires the WAN to be hub-and-spoke, or a spokeless hub in the case of a Multiprotocol Label Switching (MPLS) virtual private network (VPN). This topology ensures that call admission control, provided by the locations configuration mechanism in Unified CM, works properly in tracking the bandwidth available between any two sites in the WAN. For general guidance on topology-unaware call admission control, refer to the Cisco Collaboration System Solution Reference Network Design (SRND), available at http://www.cisco.com/go/ucsrnd.

Topology-aware Resource Reservation Protocol (RSVP) cannot be used within the cluster or between clusters as a call admission control technique. For IPv6-enabled Unified CM clusters:

- Locations-based call admission control must be used between sites controlled by the same Unified CM cluster.
• Unified CM SIP trunks support only locations-based call admission control (IPv4 and/or IPv6).

• Unified CM MGCP trunks support only locations-based call admission control (IPv4-only).

• Unified CM H.323 trunks support locations-based call admission control and gatekeeper-controlled call admission (IPv4-only).

For IPv6 traffic, Unified CM uses the values shown in Table 11: Layer 3 Bandwidth per VolIPv6 Flow, on page 59 in its locations-based call admission control algorithm.

Locations-Based Call Counting Call Admission Control

Unified CM also supports a type of locations-based, topology-unaware call admission control known as call counting. Less sophisticated than standard Unified CM locations-based call admission control, call counting uses a fixed bandwidth value for each voice and video call, irrespective of the codec or actual bandwidth used.

For call counting, the following default values are used for Layer 3 voice and video bandwidth when calculating the amount of available bandwidth at a location:

• Voice calls = 102 kbps

• Video calls = 500 kbps

Although call counting provides a simplified form of call admission control, it also has the disadvantage that bandwidth reserved for voice and video in the WAN might not be used efficiently.

To enable call counting in Unified CM Administration, select Service Parameters > Clusterwide Parameters (Call Admission Control). The default setting for Call Counting CAC Enabled is False. The voice and video bandwidth values for call counting are configurable.

Figure 43: Configuring Call Counting

Cisco Business Edition

Cisco Business Edition supports IPv4-only.
CHAPTER 10

Dial Plan

- Dial Plan Overview, on page 105
- IPv6 and Unified CM Dial Plans, on page 106
- Call Routing in Cisco IOS IPv6 Dial Peers, on page 108
- Emergency Services, on page 108

Dial Plan Overview

The dial plan is one of the key elements of a Unified Communications system, and an integral part of all call processing agents. Generally, the dial plan is responsible for instructing the call processing agent on how to route calls. Specifically, the dial plan performs the following main functions:

- Endpoint addressing
  Reachability of internal destinations is provided by assigning directory numbers (DNs) to all endpoints.

- Path selection
  Depending on the calling device, different paths can be selected to reach the same destination.

- Calling privileges
  Different groups of devices can be assigned to different classes of service, by granting or denying access to certain destinations.

- Digit manipulation
  Sometimes, it is necessary to manipulate the dialed string before routing the call.

- Call coverage
  Special groups of devices can be created to handle incoming calls for a certain service according to different rules (top-down, circular hunt, longest idle, or broadcast).

**IPv6 and Unified CM Dial Plans**

The deployment of IPv6 with Cisco Unified Communications Manager (Unified CM) affects two areas of dial plan functionality:

- IPv6 addressing for SIP route patterns
- Path selection considerations for IPv6 calls over IPv6-capable networks

**SIP IPv6 Route Patterns**

Unified CM can use SIP route patterns to route or block both internal and external calls to SIP endpoints. SIP route patterns can use the destination domain name, an IPv4 address, or an IPv6 address to provide a match for call routing.

A SIP request to call a device can take either of the following forms:

- Using an address:
  
  ```
  INVITE sip:5001@2001:0db8:2::1 5060 SIP/2.0
  ```

- Using a domain name:
  
  ```
  INVITE sip:5001@example.com 5060 SIP/2.0
  ```

To process the SIP request, the Unified CM administrator can add domains, IP addresses, and IP network addresses, and associate them to SIP trunks (only), as shown in the following figure. This method allows requests that are destined for these domains to be routed through particular SIP trunk interfaces.
The following guidelines and examples apply to SIP route patterns:

- Domain name examples:
  - example.com
  - my-pc.example.com
  - *.com
  - rtp-ccm[1-5].example.com

- Valid characters for domain names:
  [., -, 0-9, A-Z, a-z, *, and ]

- If domains names are used, then DNS must be configured in the Unified CM cluster.

- IPv4 address examples:
  - 192.168.201.119 (explicit IP host address)
• 192.168.0.0/16 (IP network)

• IPv6 address examples:
  • 2001:0db8:2::1 (explicit IPv6 host address)
  • 2001::/16 (IPv6 network)

• Valid characters for IPv6 addresses:
  0-9, A-F, :, and /

**Path Selection Considerations for IPv6 Calls**

If you create an IPv6 route pattern, then that route pattern must be associated with an IPv6-capable SIP trunk. Likewise, the campus network or WAN that the IPv6 call traverses must be IPv6-capable.

**Call Routing in Cisco IOS IPv6 Dial Peers**

The following example shows a typical Cisco IOS IPv6 dial peer. Note that Alternative Network Address Types (ANAT) has been configured on this dial peer, thus allowing either an IPv4 address or IPv6 address to be negotiated for media. The session target can be configured with only one address, either IPv4 or IPv6.

```
dial-peer voice 1 voip
description **** SIP Trunk to CUCM ****
destination-pattern 5...
voice-class sip anat
session protocol sipv2
session transport tcp
dtmf-relay rtp-nte
no vad
```

**Emergency Services**

Cisco Emergency Responder (Emergency Responder) can track the IPv6-only phones through the switch port-based tracking, or access point-based tracking, or as manually configured phones. For the switch port-based tracking, Emergency Responder can talk to Cisco switches configured as the IPv4 address or IPv6 address through the SNMP protocol. Access point-based tracking requires the IPv6-only phone to communicate its upstream infrastructure information to Unified CM. For more information on Access Point Configuration and Discovery, refer to the Cisco Emergency Responder Administration Guide.

Emergency Responder tracks registered endpoints in Unified CM and provides Emergency Call Treatment for reaching correct PSAP and with correct Location information.

Emergency Responder interfaces with the following components:

• A Unified CM cluster by the following methods:
• JTAPI, SNMP V3/V2, and AXL using IPv4 interface, to collect IPv6 information about its configured IP Phones. Emergency Responder and Unified CM are IPv6-aware.

• JTAPI, to allow for the call processing associated with redirection of the call to the proper PSAP gateway.

• The access switches (through SNMP IPv4 or IPv6) where the phones associated with Unified CM are connected. Unified CM is IPv6-aware to communicate with Emergency Responder using IPv4 transport. The Emergency Responder to Switch interface is IPv6, supporting SNMP V3/V2.

Emergency Responder Limitations for IPv6-Only Endpoints

Some limitations for IPv6-only endpoints include:

• A call coming to Emergency Responder from an analog phone must be connected to an IPv4 gateway.

• Teleworker and off-premises features work only with IPv4.
Applications

Applications Overview

All Cisco applications that can terminate voice media support IPv4-only. For these applications, if a call is extended from an IPv6-only device to the IPv4-only application, Cisco Unified Communications Manager (Unified CM) inserts a media termination point (MTP) to convert the voice media from IPv6 to IPv4, as shown in the following figure.

Figure 45: MTP Inserted for Conversion Between IPv6 and IPv4

Voicemail
Cisco Unity Connection supports IPv6 for all interfaces, and Cisco Unity Express supports IPv4 only.

LDAP Directory Integration
Unified CM supports IPv4 with Lightweight Directory Access Protocol (LDAP) for directory sync. IP Phones 8800/7800 exercise UDS (http). IP Phones use CCMPD and CCMCIP services for Personal and Corporate Directory. These services are IPv6 compliant. Back-end interfaces from Unified CM to AD are not validated for IPv6, and should be IPv4-only.
Native Unified CM Applications
Cluster-wide Extension Mobility, IP Phones Services, Cisco Unified Communications Manager Assistant, Cisco Unified Communications Attendant Console, MRA, and Web Dialer support IPv4-only.

Video Conferencing
Cisco Meeting Server and Cisco TelePresence Management Suite (TMS) for video conference support is in a traditional IPv4 stack. IPv4 or IPv6 endpoints are supported in a cluster. Any IPv6-only endpoint can join Cisco Meeting Server video conference service. Additional MTP is required in Unified CM to provide media inter-working IPv4 to IPv6.

Multistream Video
Multistream video that allows an IPv4 or IPv6 endpoint to send multiple resolution video streams is supported. The bridge passes the most appropriate streams to the far-end video units that can be IPv4 or IPv6 stack. The far end video unit receives a full resolution stream of the active speakers.

Device Mobility
Device Mobility is supported only for IPv4-only, IPv6-only, and dual-stack devices.

Unified CM IM and Presence Service
Cisco Unified Communications Manager IM and Presence Service (IM and Presence Service), Cisco IM and Presence Service Client, and Cisco IP Phone Messenger support dual-stack or IPv6-only.

Cisco Mobility Applications
Mobility applications support IPv6-only.

Cisco Jabber Applications
Cisco Jabber applications support IPv6-only for desktop on-premise application deployments only. For MRA, Jabber should be configured for dual-stack (with IPv6 preferred) because of the IPv6-only support limitation in Cisco Expressway. In this dual-stack, ANAT as media is not applicable; it is for applications server interface only based on RFC 6555. Jabber applications in Android and iOS 3G/4G mobile networks will support IPv6 because of a NAT64 solution developed by mobile network service providers. In an off-premise deployment, we recommend Jabber dual-stack due to users roaming in various service provider networks.

Cisco Unified Survivable Remote Site Telephony
Cisco Unified Survivable Remote Site Telephony (Unified SRST) functions as a dual-stack application server that supports the following devices, which have IP phone line side feature such as: Hold/Resume, Forwarding, 3WC, Transfer, MOH, ATA Fax in IPv4 mode:

- Unified SRST 12.0 supports the following Cisco IP Phones for voice only services in IPv6-only addressing mode using SIP signaling based on the ISR 4K Routers:
  - Support for Cisco IP Phone 7811, 7821, 7841 and 7861
  - Support for Cisco IP Phones 8811, 8841, 8845, 8851, 8861, and 8865
  - Not supported endpoints: Jabber and SCCP IP Phones
• Unified SRST 12.0 will not support SCCP signaling and SIP SDP ANAT dual-stack attributes to support media selection that can be IPv4 or IPv6.
  
  • All the legacy dual-stack phones default to IPv4-only SIP mode in Unified CM.
  
  • PSTN gateways are configurable to SIP IPv4-only or IPv6-only. This gateway supports incoming, outgoing, and emergency calls to service provider PSTN.

• Media Inter-working: Unified SRST provides IPv4 to IPv6 RTP media inter-working for voice and video endpoints. This media inter-working is required when using IPv6-only endpoints, or when gateways are configured to IPv4-only mode.

For more information, refer to the Cisco Unified SCCP and SIP SRST System Administrator Guide.
IP Video Telephony Overview

IPv6 transition will follow Cisco Preferred Architecture deployment recommendations of IPv4. Cisco Unified Communications Manager (Unified CM) is the call control server for the Cisco Preferred Architecture for Enterprise Collaboration deployment. Cisco IP Phones, Cisco Jabber clients, and Cisco TelePresence video endpoints use SIP to register directly to Unified CM. The Unified CM cluster’s failover mechanism provides endpoint registration redundancy. If a WAN failure occurs and endpoints at remote locations cannot register to Unified CM, they use SRST functionality for local and PSTN calls, but some services such as voicemail and presence might not be available.

Although we have not tested these, the Cisco DX Series, and Cisco TelePresence MX, SX, and IX5000 Series products that are specified in the Preferred architecture document are available to you for lab testing in IPv6-only mode. The major gap in testing is support of DHCP IPv6. You will need to configure all the products manually with IPv6 addresses. This solution testing is limited to on-premise devices without MRA support. Cisco Expressway does not support IPv6. Various video conference solutions including Cisco TelePresence Management Suite are out of scope for lab testing and remain in IPv4 addressing mode.

In CSR 12.0, IP video telephony was not solution tested for IP Phones, TelePresence endpoints, and conferencing components and is not supported. You can work with your Cisco account team for lab testing guidelines at your location.
Video calls can be made across ANAT-enabled dual-stack SIP trunks that are configured to use Delayed Offer. Usually, both the voice and video streams for these calls use IPv4.
CHAPTER 13

IP Telephony Migration Options

• IP Telephony Migration Options Overview, on page 117

IP Telephony Migration Options Overview

For first-time installations of IPv6 with Cisco Unified Communications Manager (Unified CM) or an upgrade to a traditional deployment, we recommend the following guidelines:

Deployment Models

For Cisco Unified CM IPv6 is supported for single-site deployments, multi-site deployments with distributed call processing, and multi-site deployments with centralized call processing. Minimum IPv6 deployment requires the following products:

• Dual-stack IPv6 Unified CM server
• MTP for media interworking
• IPv6-only IP Phones

All other components and interfaces can remain in IPv4. Unified CM will insert MTPs to provide media interworking for various use cases.

Campus Network and WAN

Before you enable IPv6 in the Unified CM cluster, make sure that both the campus network and the WAN support both IPv4 and IPv6 traffic. Dual-stack (IPv4 and IPv6) routing is recommended for Layer 3 campuses and WANs.

Cluster-Wide IPv6 Configuration Settings

To maximize the amount of IPv6 traffic on your Unified Communications network, use the following settings for the cluster-wide IPv6 Enterprise Parameters:

• Enable IPv6: True
• IP Addressing Mode Preference for Media: IPv6
• IP Addressing Mode Preference for Signaling: IPv6
**Common Device Configuration Profiles**

Use multiple Common Device Configuration Profiles so that individual phones and trunks or groups of phones and SIP trunks can be selectively configured to support IPv6.

The Common Device Configuration Profile in Unified CM Administration (Device > Device Settings > Common Device Configuration) contains the following IPv6 configuration information:

- IP Addressing Mode
- IP Addressing Mode Preference for Signaling
- Allow Stateful Auto-Configuration for Phones

**DHCP**

Stateful DHCPv6 is recommended, although stateless DHCP can also be used with Stateless Address Auto-Configuration (SLAAC) for phones.

**MTPs**

For multi-site distributed call processing deployments, you will most likely need to use Cisco IOS media termination points (MTPs) for conversions between IPv4 and IPv6. These MTPs should be associated with both phone and SIP trunk media resource groups (MRGs).

**IPv6 SIP Trunks**

IPv6 SIP trunks should be configured as Delayed Offer without Alternative Network Address Types (ANAT) enabled. However, SIP trunks configured for Early Offer (MTP Required) using an MTP resource for every call are do not support video calls or encrypted calls.

**IP Phones**

IPv6-only phone support is a major feature of CSR 12.0, as it helps to mitigate IPv4 exhaustion. We recommend that you configure all IP Phones as IPv6-only where applicable. All other IP Phones must be configured as IPv4. Dual-stack IP Phones require ANAT which is not supported in Unified SRST call agents.

**ISDN PSTN Gateway and SRST ISR 4000**

To transition to an IPv6-only network and to reduce the MTP requirements, configure ISDN PSTN gateways and SRST ISR 4000 with Delay Offered SIP IPv6-only trunk.
Security

- Security Overview, on page 119
- Privacy and Encryption for IPv6 Voice Signaling and Media, on page 119
- Encrypted Media and MTPs Between IPv4 and IPv6, on page 120
- CAPF and CTL, on page 121
- IPv6 Collaboration Traffic and Firewalls, on page 121
- Cisco Unified Border Element, on page 122
- Security and IPv6 Traffic, on page 122

Security Overview

When comparing IPv4 and IPv6 in terms of how secure each protocol is, IPv6 has some advantages and some disadvantages, but overall it is no more or less secure than IPv4. One inherent benefit of IPv6 is the enormous size of IPv6 subnets and networks, which offer improvements in protection against automated scanning and worm propagation. Typical security drawbacks are the addressing complexity of IPv6 and the likelihood that network administrators will not be familiar with the IPv6 protocol and IPv6 security tools.

In general, most of the legacy issues with IPv4 security remain in IPv6. For example, Address Resolution Protocol (ARP) security issues in IPv4 are replaced with neighbor discovery (ND) security issues in IPv6. In CSR 12.0, IPv6 security settings have the same functionality as IPv4, such as Firewall, sRTP and TLS.

Privacy and Encryption for IPv6 Voice Signaling and Media

This was not solution tested for voice service in CSR 12.0.

The Internet Engineering Task Force (IETF) and RFCs 4301-4303 mandate authentication and encryption for IPv6 using IP Security (IPsec). However, to avoid interworking issues with legacy IPv4 Unified Communications endpoints, Cisco Unified Communications Manager (Unified CM) IPv4 and IPv6 deployments continue to use Transport Layer Security (TLS) and Secure Real-Time Transport Protocol (SRTP) for authentication and encryption between IP phones and between IP phones and SIP gateways and trunks.

IPsec can also be used for IPv4-based H.323 and Media Gateway Control Protocol (MGCP) gateway connections.
Cisco Unified CM provides the following secure transport protocols:

- **Transport Layer Security (TLS)**
  
  TLS provides secure and reliable data transfer between two systems or devices by using secure ports and certificate exchange. TLS secures and controls connections between Unified CM-controlled systems, devices, and processes to prevent access to the voice domain. Unified CM uses TLS to secure Skinny Client Control Protocol (SCCP) calls to phones that are running SCCP, and to secure SIP calls to phones or trunks that are running SIP.

- **IP Security (IPsec)**
  
  IPsec provides secure and reliable data transfer between Unified CM and gateways. IPv4-based IPsec implements signaling authentication and encryption to Cisco IOS MGCP and H.323 gateways.

You can add Secure Real-Time Transport Protocol (SRTP) to TLS and IPsec transport services for the next level of security on devices that support SRTP. SRTP authenticates and encrypts the media stream to ensure that voice conversations originating or terminating on Cisco Unified IP Phones and either TDM or analog voice gateway ports, are protected from eavesdroppers who might have gained access to the voice domain. SRTP adds protection against replay attacks.

For more information on Unified CM security, refer to the *Cisco Unified Communications Manager Security Guide*, available at:


### Encrypted Media and MTPs Between IPv4 and IPv6

Unified CM supports encrypted calls between dual-stack (IPv4 and IPv6) and single-stack (IPv4 or IPv6) devices. If an IP addressing version mismatch exists between the called and calling device, Unified CM dynamically inserts an MTP to convert the IP header of the encrypted voice stream. This dynamically inserted MTP uses its pass-through codec for the encrypted media stream and changes only the IP headers from IPv4 to IPv6 and conversely.
CAPF and CTL

Certificate Authority Proxy Function (CAPF) supports both IPv4 and IPv6 addressing and uses TCP/IP to communicate with phones and to perform its standard security certificate functions. In an IPv6-enabled Unified CM cluster, CAPF has the following capabilities:

- Issuing and upgrading certificates to IPv4-only IP phones
- Issuing and upgrading certificates to IPv6-only IP phones
- Issuing and upgrading certificates to dual-stack (IPv4 and IPv6) IP phones

No new IPv6 functionality is needed for Certificate Trust List (CTL).

IPv6 Collaboration Traffic and Firewalls

The Cisco Adaptive Security Appliance (ASA) supports SCCP or SIP for IPv6, therefore can be used to open pinholes dynamically for IPv6 voice traffic. This product supports basic firewall and traffic filtering function for IPv6 traffic.

If you want to implement basic firewall capability for IPv6, refer to the following documents:
Cisco Unified Border Element

The Cisco IOS-based ISR 4000 G3 Cisco Unified Border Element can:

• Terminate a SIP IPv6 call on one leg of a session, and generate a SIP IPv4 call on the other leg.
• Terminate a SIP IPv6 call on one leg of a session, and generate a SIP IPv6 call on the other leg.

This functionality allows for basic interconnection between enterprise IPv6 networks and service provider IPv4 networks.

Basic calls with both media and signaling processing are supported. Basic Supplementary Services over IPv6 are supported, but H.323 IPv6 calls are not supported.

Security and IPv6 Traffic

Future releases of the Cisco security platforms and products mentioned in this chapter will support IPv6 collaboration traffic. However, until these products do support IPv6 for collaboration traffic, we recommend that you keep all IPv6 voice traffic within your enterprise network.

If you want to use firewalls within your campus network (for example, to secure Unified CM, centralized media resources, and other voice applications), then change the Unified CM IP Addressing Mode Preference for Signaling to IPv4 to allow inspection for all SCCP and SIP signaling traffic. As an alternative, you can use access control lists (ACLs) to open the firewall for IPv6 traffic.
Collaboration Endpoints

IPv6 Capabilities of Collaboration Endpoints

This chapter describes a subset of the Cisco Collaboration endpoints and their IPv6 capabilities. The following table lists the endpoint types and summarizes their IPv6 capabilities. IPv6 support extends to only a subset of the Cisco analog gateways and IP phones. The following sections discuss these devices in more detail.

**Table 17: IPv6 Capabilities of Collaboration Endpoints**

<table>
<thead>
<tr>
<th>Endpoint Type</th>
<th>IPv6 Capability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Analog gateways</td>
<td>ISR 4000 does not support Cisco VG Series Gateways for IPv6-only.</td>
</tr>
<tr>
<td>Cisco IP Phones</td>
<td>CiscoUnified IP Phones 7800 and 8800 Series support IPv6-only.</td>
</tr>
<tr>
<td>Software-based endpoints</td>
<td>Jabber software-based endpoints support IPv6.</td>
</tr>
<tr>
<td>Wireless endpoints</td>
<td>No wireless endpoints support IPv6.</td>
</tr>
<tr>
<td>Cisco Unified IP Conference Station</td>
<td>Conference stations support IPv6.</td>
</tr>
<tr>
<td>Cisco TelePresence video endpoints (CE software)</td>
<td>Not solution tested.</td>
</tr>
<tr>
<td>Third-party SIP IP phones</td>
<td>Third-party IPv6-capable phones are not supported.</td>
</tr>
</tbody>
</table>

IPv6 Support on Cisco IP Phones

For a list of the CSR 12.0 endpoints that support IPv6-only, see Recommended IPv6 Addressing Modes for CSR 12.1/12.0 Products, on page 20. Any endpoints not listed there should be configured in IPv4-only stack.

When a phone with a single IPv4 address needs to communicate with a phone with a single IPv6 address, an IP addressing version incompatibility exists. To resolve this media addressing incompatibility, Unified CM
dynamically inserts a media termination point (MTP) to convert the media stream from IPv4 to IPv6 (and conversely).

**IP Phone Deployment Considerations in an IPv6 Network**

The **PC Voice LAN Access** setting on IP phones is typically used to allow the monitoring of IP phone traffic by monitoring and recording applications and by network monitoring software. This setting also allows multicast traffic to be propagated from the voice VLAN to the IP phone's PC port. By default, the PC Voice VLAN Access setting is enabled on IP phones.

In IPv6-enabled networks, this default PC Voice VLAN Access setting allows Router Advertisement (RA) multicast messages to be sent from the voice VLAN to the IP phone's PC port. Ordinarily, the PC should drop any packets that it receives with a voice VLAN tag because it is not configured for the voice VLAN and does not understand 802.1g tagging. However, if the PC does accept packets with a voice VLAN tag and uses an RA from the voice VLAN, it can cause an IPv6 address from the voice VLAN to be assigned to the PC.

If you encounter the issue of incorrect IPv6 address assignment for PC port devices, use either of the following techniques to resolve this issue:

- Set the prefix lifetime of RAs sent by routers in the voice VLAN to a shorter lifetime value than the RAs sent by routers in the data VLAN, and also ensure that routers in the data VLAN have higher priority than those in the voice VLAN. IPv6 devices in the data VLAN using the Address Selection Algorithm (RFC 3484) choose the Network Prefix included in RAs with the longest lifetime, and thus prefer routers in the data VLAN.

- For all IP phones with connected devices that are affected by the above issue, set the IP phone's PC Voice VLAN Access setting to disabled. For large numbers of phones, this configuration change can be bulk-provisioned through the Unified CM Bulk Administration Tool (BAT).

**Common Device Configuration Profile**

The process for configuring IPv6 on the phones is similar to that for SIP trunks. In Cisco Unified CM Administration, select **Device > Device Settings > Common Device Configuration** to create and configure a Common Device Configuration Profile and associated it with one or more IP phones. The Common Device Configuration Profile contains the following IPv6 configuration information:

- IP Addressing Mode
- IP Addressing Mode Preference for Signaling
- Allow Auto-Configuration for Phones

**IP Addressing Mode**

The phone IP Addressing Mode has three settings:

- **IPv4 Only**
  
  In this mode, the phone acquires and uses only one IPv4 address for all signaling and media. If the phone has previously acquired an IPv6 address, it releases that address.

- **IPv6 Only**
In this mode, the phone acquires and uses only one IPv6 address for all signaling and media. If the phone has previously acquired an IPv4 address, it releases that address.

- IPv4 and IPv6

In this mode, the phone acquires and uses one IPv4 address and one IPv6 address. It can use the IPv4 and the IPv6 address as required for media. It uses either the IPv4 address or the IPv6 address for call control signaling to Unified CM.

If IPv6 is enabled in the Unified CM cluster, the default phone setting for IP Addressing Mode is IPv4 and IPv6. If the IP phone supports both IPv4 and IPv6, it will adopt this setting, but all IPv4-only phones will ignore this setting.

We recommend setting the phone IP Addressing Mode to IPv4 and IPv6. A setting of IPv6 Only is not recommended and should be used only in test environments. For more information on IPv6-only phone functionality, see IPv6-Only Phones, page 15-7.

**IP Addressing Mode Preference for Signaling**

The phone IP Addressing Mode Preference for Signaling has three settings:

- IPv4
  If the phone has an IPv4 address, it uses that IPv4 address for call control signaling to Unified CM.

- IPv6
  If the phone has an IPv6 address, it uses that IPv6 address for call control signaling to Unified CM.

- Use System Default
  In this case, the phone uses the cluster-wide Enterprise Parameter configuration value for its IP Addressing Mode for Signaling.

If IPv6 is enabled in the Unified CM cluster, the default phone setting for IP Addressing Mode for Signaling is Use System Default. If the IP phone supports either IPv6 or both IPv4 and IPv6, it will adopt the cluster-wide setting for IP Addressing Mode for Signaling, but all IPv4-only phones will ignore this setting.

**Allow Auto-Configuration for Phones**

Allow Auto-Configuration for Phones has three settings:

- On

  With this setting, the phone is allowed to use Stateless Auto Address Configuration (SLAAC) to acquire an IPv6 address. Whether or not the phone uses SLAAC depends on the link-local router’s O and M bit configuration for router advertisements (RAs), as follows:

  - If the O bit is set in the router's RAs, the phone uses SLAAC to acquire an IPv6 address and uses the DHCP server to acquire other information such as the TFTP server address.
  - If the M bit is set in the router’s RAs, the phone does not use SLAAC. Instead, it uses the DHCP server to acquire its IP address and other information (Stateful DHCP).
  - If neither the M bit nor the O bit is set, the phone uses SLAAC to acquire an IP address and does not use DHCP for other information. The phone also requires a TFTP server address to download its configuration file and register to Unified CM. This TFTP server address can be configured manually through the phone’s user interface (UI).
• Off

With this setting, the phone does not use Stateless Auto Address Configuration (SLAAC) to acquire an IPv6 address. In this case, the phone can either be configured manually or use Stateful DHCPv6 to acquire an IPv6 address and TFTP server address.

• Default

With this setting, the phone uses the cluster-wide Enterprise Parameter configuration value for Allow Auto-Configuration for Phones.

Default Common Device Configuration Profile

By default, there are no Common Device Configuration profiles configured, and each device is associated with a <None> Common Device Configuration. If IPv6 is enabled in the Unified CM cluster with this default configuration, IPv6-capable devices adopt the following settings:

• IP Addressing Mode = IPv4 or IPv6
• IP Addressing Mode Preference for Signaling = Use System Default
• Allow Auto-Configuration for Phones = Default

Figure 48: Effect of IP Addressing Mode for Media on MTP Usage for IP Phones

Other IP Phone Functions

The following functions also affect the use of IPv6 on Cisco IP Phones.

TFTP

As previously described, TFTP servers support both IPv4 and IPv6 addresses. IPv4-only phones use their received IPv4 TFTP address to reach the TFTP server, and IPv6-only phones use their received IPv6 TFTP address to reach the TFTP server. Dual-stack phones can use either their IPv4 or IPv6 TFTP address to reach the TFTP server.
The following IPv6 information is sent to the phone in its configuration file from the TFTP server:

- Unified CM IPv4 and IPv6 addresses
- The setting for IP Addressing Mode
- The setting for IP Addressing Mode Preference for Signaling
- The setting for Allow Stateless Auto-Configuration for Phones

**Unified CM Registration for Dual-Stack IP Phones**

Dual-stack phones attempt to connect to Unified CM by using the preferred (IPv4 or IPv6) address specified in the IP Addressing Mode Preference for Signaling parameter found in the TFTP configuration file. If the first attempt at connection fails due to a TCP timeout, the phone then attempts to connect to Unified CM using its other address.

**IP Phone HTTP Server Functionality**

The HTTP server function of all IP phones uses IPv4-only or IPv6-only. The HTTP server provides several functions, including:

- Phone User Interface access to:
  - Directory search functions
  - Call history
  - All IP Phone Services
  - Extension Mobility
  - IPv4-only supported Quality Report Tool (QRT)

- Web access to the phone through the Unified CM phone administration graphical user interface

**CDP and LLDP**

IP phones support the sending and receiving of IPv4 and IPv6 addresses in data link layer Cisco Discovery Protocol (CDP) and Link Layer Discovery Protocol (LLDP) messages. Currently, Cisco applications do not use any of the IPv6 addresses sent in LLDP messages. CDP is applicable to Emergency Responder and discovery of a desk phone device.

**IPv6-Only Phones**

IP phones configured with an IP addressing mode of IPv6-only are subject to a number of functional limitations that must be evaluated before any production network deployments. Those limitations are described here:

- The following functions are not available to IPv6-only phones:
  - EMCC
  - NTPv6
• Peer Firmware Sharing (PFS) for the distribution of files between like phones is not supported for IPv6-only phones. IPv6-capable phones do support a load server using an IPv6 address.

• CAST Protocol for Jabber, Establish and maintain a connection to the desk phone device

• MRA

• Power Save Plus (EnergyWise), need Switch support (No future plan, deprecated by switch)

• VPNv6

• IPv6-only Out-of-Band and Boot

• IPv6 multicast (MOH), Unified CM does not support IPv6 multicast MOH (Not a solution requirement)

• Device mobility uses IP subnet information to locate mobile devices and this function is not supported for IPv6-only phones.
Appendix

- Product Configuration Resources for IPv6, on page 129
- Document Direction, on page 130
- Deprecation of ANAT SIP SDP Attributes, on page 131

Product Configuration Resources for IPv6

To configure CSR 12.1/12.0 products for IPv6, refer to the product configuration guides.

Table 18: CSR 12.1/12.0 Endpoints

<table>
<thead>
<tr>
<th>Endpoint (SIP)</th>
<th>IPv6 Configuration Resources</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IP Phone 7800 Series</td>
<td>Administration Guides</td>
</tr>
<tr>
<td>Cisco IP Phone 8800 Series</td>
<td>Administration Guides</td>
</tr>
<tr>
<td>Cisco Jabber</td>
<td>On-Premises Deployment Guide</td>
</tr>
<tr>
<td>Cisco DX70 and DX80 (CE endpoints)</td>
<td>Support</td>
</tr>
<tr>
<td>Cisco TelePresence MX Series (CE endpoints)</td>
<td>Support</td>
</tr>
<tr>
<td>Cisco TelePresence SX Series (CE endpoints)</td>
<td>Support</td>
</tr>
<tr>
<td>Cisco TelePresence EX Series (CE endpoints)</td>
<td>Support</td>
</tr>
</tbody>
</table>

Table 19: CSR 12.1/12.0 Communication Gateways

<table>
<thead>
<tr>
<th>Gateway</th>
<th>IPv6 Configuration Resources</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco 4000 Series Integrated Services Routers (ISR)</td>
<td>Configuration Guides</td>
</tr>
<tr>
<td>Cisco 2900 and 3900 Series Integrated Services Routers (ISR) (For CUBE)</td>
<td>CUBE Configuration Guide</td>
</tr>
</tbody>
</table>
### Document Direction

This document is based Collaboration IP endpoints being dual-stack, which was driven by the DoD requirements, where IPv4 exhaustion was not the driver to deploy IPv6. DoD's direction was to roll out IPv6 slowly, not to have IPv6-only networks. To reduce IPv4 and IPv6 media inter-working (MTP), each endpoint was implemented with both IPv4 and IPv6 addresses using SIP SDP attributes of ANAT. For enterprise networks, it was not acceptable to assign IPv4 addresses to IPv6 devices. Their expectation was to assign only IPv6 addresses in all deployment use cases.

Starting in CSR 12.0, we recommend deploying IPv6-only device configuration where applicable, typically endpoints and PSTN gateways. All applications servers need IPv4 address and IPv6 address (dual-stack) to support all traditional IPv4 devices until all devices are IPv6-only capable including third-party products and applications.

This document includes the current ANAT configuration information that is not solution tested and TAC supported in CSR 12.1/12.0. The Unified CM and DoD default values are the same as shown in various configuration tabs.

We will update this document in the future based on the market requirements and approval by DoD to deprecation of the ANAT RFCs 4091 and 4092. The Unified CM configuration tabs will be updated accordingly with new default values of IPv6 in the next major release.
To reduce dependency on IPv4 addresses, you can upgrade the following on-premise deployment modes to IPv6: single-site call processing deployments; multi-site distributed call-processing deployments; and multi-site deployments with centralized call processing. We recommend that you upgrade and configure:

- IPv6-only stack SIP phones, SIP gateways, and SIP trunks.
- IPv4-only stack and IPv6-only stack (dual-stack) Unified CM clusters and other application servers.
- All third-party products and applications in IPv4-only.

### Deprecation of ANAT SIP SDP Attributes

Department of Defense (DoD) certification requirements drove the development of Alternative Network Address Types (ANAT) RFC 4091 and 4092. ANAT allows a set of network addresses to establish a media stream is useful in environments with both IPv4-only hosts and IPv6-only hosts. For this functionality, all the devices need IPv4 address and IPv6 address assignment. ANAT was also implemented in Cisco Unified Communication System Release 7.1.2. However, since all device need both IPv4 and IPv6 addresses, ANAT does not help to reduce dependency on the now depleted number of IPv4 addresses. Based on large enterprise customer feedback, and their need for new IP addresses, ANAT SIP SDP attributes have since been deprecated by Internet Engineering Task Force (IETF).

Starting with CSR 12.0, we recommend deploying IPv6-only device configuration where applicable (typically endpoints). All servers, third-party products, and applications need IPv4 addresses and IPv6 addresses to support all traditional IPv4 devices until all devices are IPv6-only capable.