# Deploying IPv6 in Unified Communications Networks with Cisco Unified Communications Manager 8.0(*x*)

June 08, 2010

**Americas Headquarters**
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-19142-02

*Deploying IPv6 in Unified Communications Networks with Cisco Unified Communications Manager 8.0(x)*

# CONTENTS

# Preface

**Revised: June 08, 2010, OL-19142-02**

This document provides design considerations and configuration guidelines for deploying IPv6 in a Cisco Unified Communications System.

This document should be used in conjunction with other documentation available at the following locations:

- For more information about the Cisco Unified Communications System:

  http://www.cisco.com/go/unified-techinfo

  http://www.cisco.com
- For more information about Cisco Unified Communications Manager (Unified CM):

  http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_series_home.html

  http://www.cisco.com
- For other Cisco Unified Communications Solution Reference Network Design (SRND) documents:

  http://www.cisco.com/go/ucsrnd
- Other Cisco design guides:

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

**Note** Unless stated otherwise, the information in this document applies to Cisco Unified Communications Manager (Unified CM) 8.*x* releases.

# Revision History

This document may be updated at any time without notice. You can obtain the latest version of this document online at:

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

Visit this Cisco.com website periodically and check for documentation updates by comparing the revision date (on the front title page) of your copy with the revision date of the online document.

The following table lists the revision history for this document.

| Revision Date | Comments |
|---|---|
| June 08, 2010 | Document revised to add a new IPv6 deployment model introduced with Cisco Unified Communications Manager 8.0. |
| May 22, 2009 | Initial release of this document. |

# Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

# Cisco Product Security Overview

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

Further information regarding U.S. export regulations may be found at:

http://www.access.gpo.gov/bis/ear/ear_data.html

CHAPTER 1

# Introduction

**Revised: June 08, 2010; OL-19142-02**

Cisco has taken a leading role in the definition and implementation of the IPv6 architecture within the Internet Engineering Task Force (IETF) and continues to lead the industry in IPv6 development and standardization.

This document describes Cisco's implementation of IPv6 for its Unified Communications products, and it discusses how to design Unified Communications networks to use IPv6 in a dual-stack (IPv4 and IPv6) environment. This document does not discuss the implementation of IPv6 in the campus and WAN in detail because these topics are discussed in other Cisco documents (which are referenced in this document). For those who are unfamiliar with IPv6, this document also provides a brief introduction to IPv6 architecture and functionality. Recommendations for further reading on IPv6 are also made in this document.

The primary focus of this document is on new IPv6 functionality for Cisco Unified Communications networks. The co-existence of IPv4 and IPv6 devices is considered throughout this document. However, Cisco strongly recommends that you use this document in conjunction with the *Cisco Unified Communications SRND*, available at

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

The *Cisco Unified Communications SRND* provides in-depth guidance on Unified Communications deployments using IPv4

The deployment of IPv6-only devices is discussed in this document, but emphasis is given to the deployment of dual-stack (IPv4 and IPv6) devices, which offer a greater degree of functionality and interoperability with existing IPv4-only devices.

**Note** The scope of this document is limited to the solutions that have been tested and approved by Cisco. Supported IPv4 applications are limited to those stated in this document. It is assumed that devices running in dual-stack mode (IPv4 and IPv6) will work with all other IPv4 applications; however, those applications that have not been tested by Cisco are not supported by Cisco Technical Assistance Center (TAC).

# Deployment Recommendations

Cisco recommends that you deploy IPv6 in a dual-stack Cisco Unified Communications Manager (Unified CM) cluster with approved dual-stack devices (phones, gateways, and so forth). This approach is recommended to avoid IPv6-only deployments, which are not currently supported in production environments. Single-site call processing deployments, multiple-site distributed call processing deployments, and multiple-site deployments with centralized call processing are supported.

To maximize IPv6 traffic in the Unified Communications network, IPv6-capable phones, SIP gateways, and SIP trunks should be configured as dual-stack devices and use IPv6 signaling and IPv6 media. SIP trunks should also be configured to use Alternative Network Address Types (ANAT).

IPv6-only Unified Communications clusters in which no IPv4 addresses are assigned to any Unified Communications components, are not supported. If IPv6-only functionality is configured, it extends to IPv6-only SIP trunks and IPv6-only IP phones (where only basic voice services are supported).

# Comparison of IPv4 and IPv6

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

## Why Deploy IPv6?

The deployment of IPv6 is primarily driven by IPv4 address space exhaustion. As the worldwide usage of IP networks increases, the number of applications, devices, and services requiring IP addresses is rapidly increasing. Current estimates by the Internet Assigned Numbers Authority (IANA) and Regional Internet Registries (such as ARIN, LACNIC, and APNIC) indicate that their pools of unallocated IPv4 addresses will be exhausted sometime between Q4 2011 and Q2+ 2012.

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.

The process of 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.

Some countries such as Japan are aggressively adopting IPv6 today. Others, such as those in the European Union, are moving toward IPv6, while China is considering building pure IPv6 networks from the ground up. Even in North America, where Internet addresses are abundant, the U.S. Department of Defense mandated that as of October 1, 2003, all new equipment purchased must be IPv6-capable. As these examples illustrate, IPv6 enjoys strong momentum.

## Advantages of IPv6 Over IPv4

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

- Larger address space

  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

  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)

  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

  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

  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

  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 Unified Communications components.

- Network-layer security

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

Table 1-1 summarizes the differences between IPv4 and IPv6.

***Table 1-1 A Comparison of IPv6 and IPv4 Services***

| IP Service | IPv4 Feature | IPv6 Feature |
|---|---|---|
| Address range | 32-bit, Network Address Translation (NAT) | 128-bit, multiple scopes |
| Auto-configuration | DHCP | Stateless, Easy Reconfiguration, DHCP |
| Routing | RIP, OSPFv2, IS-IS, EIGRP, MP-BGP | RIPng, OSPFv3, IS-IS, EIGRP, MP-BGP |
| IP Security | IPSec | IPSec |
| Mobility | Mobile IP | Mobile IP with direct routing |

*Table 1-1 A Comparison of IPv6 and IPv4 Services (continued)*

| IP Service | IPv4 Feature | IPv6 Feature |
|---|---|---|
| Quality of Service (QoS) | Differentiated Service, Integrated Service | Differentiated Service, Integrated Service |
| IP multicast | IGMP, PIM, and Multicast BGP | MLD, PIM, and Multicast BGP; Scope Identifier |

CHAPTER 2

# IPv6 Basics

**Revised: June 08, 2010; OL-19142-02**

This chapter provides an introduction for those who are unfamiliar with IPv6 addressing and IPv6 services. The basics of IPv6 addressing are discussed, as are the various address types, address assignment options, new DHCP features, and DNS. For further reading on IPv6, refer to the following documentation:

- *Deploying IPv6 Networks*, a Cisco Press publication available through http://www.cisco.com/web/about/ac123/ac220/about_cisco_cisco_press.html
- *Implementing Cisco IPv6 Networks*, a Cisco Press publication available through http://www.cisco.com/web/about/ac123/ac220/about_cisco_cisco_press.html
- Other Cisco online documentation at 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

Leading zeros can be omitted, and consecutive zeros in contiguous blocks can be represented by a double colon (::). Double colons can appear only once in the address. For example:

2001:0db8:0000:130F:0000:0000:087C:140B can be abbreviated as

2001:0db8:0:130F::87C:140B

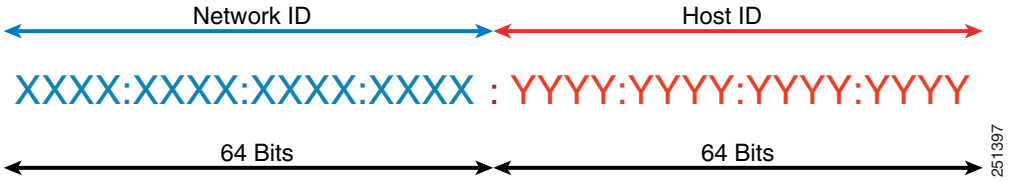
As with the IPv4 Classless Inter-Domain Routing (CIDR) network prefix representation (such as 10.1.1.0/24), an IPv6 address network prefix is represented the same way:

2001:db8:12::/64

# 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, as illustrated in Figure 2-1.

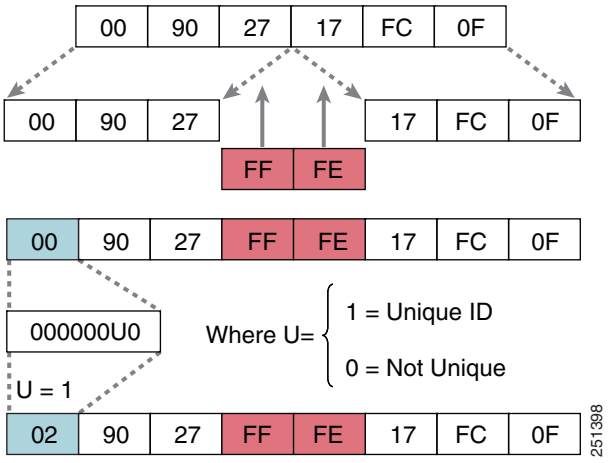
***Figure 2-1 IPv6 Unicast Network and Host ID Format***




The network ID is administratively assigned, and the host ID can be 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. This format expands the device interface 48-bit MAC address to 64 bits by inserting FFFE into the middle 16 bits (see Figure 2-2). Cisco commonly uses the EUI-64 host ID format for Cisco IP Phones, gateways, routers, and so forth.

***Figure 2-2 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. The IPv6 addresses assigned to an interface can be any of the following 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

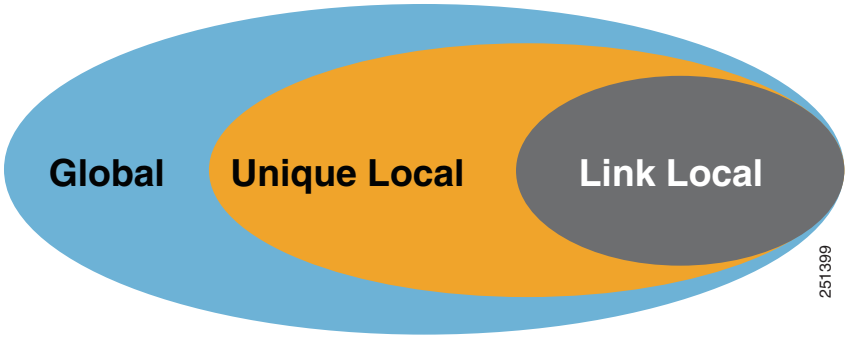
  Identifies a group of nodes or interfaces. Traffic destined to an anycast address is forwarded to the nearest node in the group. An anycast address is essentially a unicast address assigned to multiple devices with a host ID = 0000:0000:0000:0000. (Anycast addresses are not widely used today.)

With IPv6, broadcast addresses are no longer used. Broadcast addresses are too resource intensive, therefore 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 (see Figure 2-3).

***Figure 2-3 IPv6 Address Scopes***



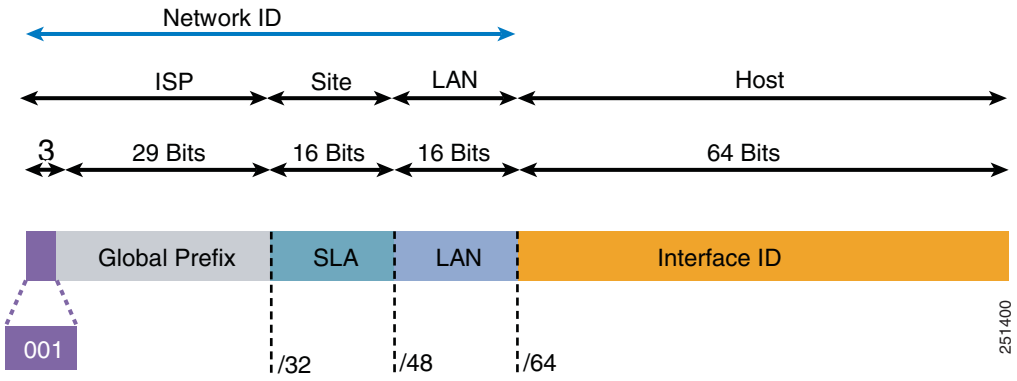

# Global Unicast Addresses

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)

Figure 2-4 illustrates the format of a global unicast address.

*Figure 2-4 Global Unicast Address Format*




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 of a global unicast address:

2001:0DB8:BBBB:CCCC:0987:65FF:FE01:2345

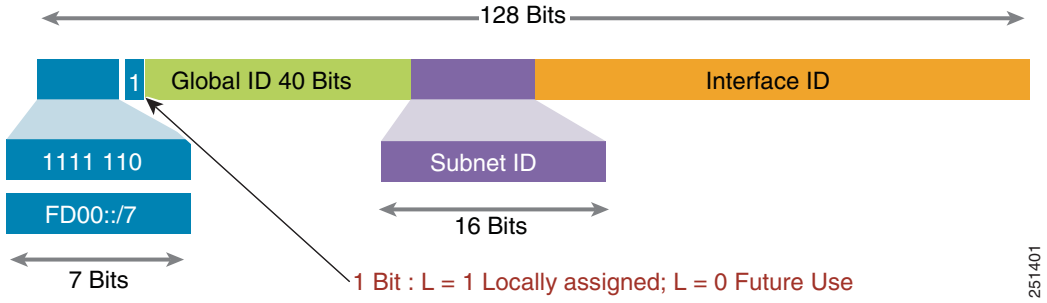
# Unique Local Unicast Addresses

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)

Figure 2-5 illustrates the format of a unique local unicast address.

*Figure 2-5 Unique Local Unicast Address Format*




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.

Example of a unique local unicast address:

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

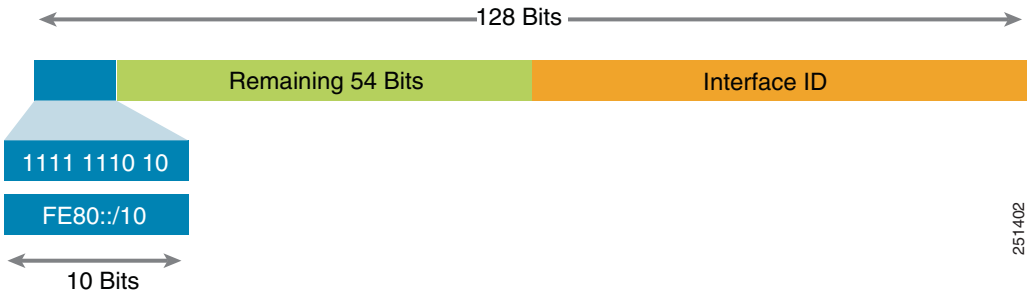
# Link Local Unicast Addresses

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 as soon as IPv6 is enabled
- Not routable addresses (Their scope is link-specific only.)
- Identified by the first 10 bits (FE80)

Figure 2-6 illustrates the format of a link local unicast address.

***Figure 2-6 Link Local Unicast Address Format***




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 of a link local unicast address:

FE80:0000:0000:0000:0987:65FF:FE01:2345

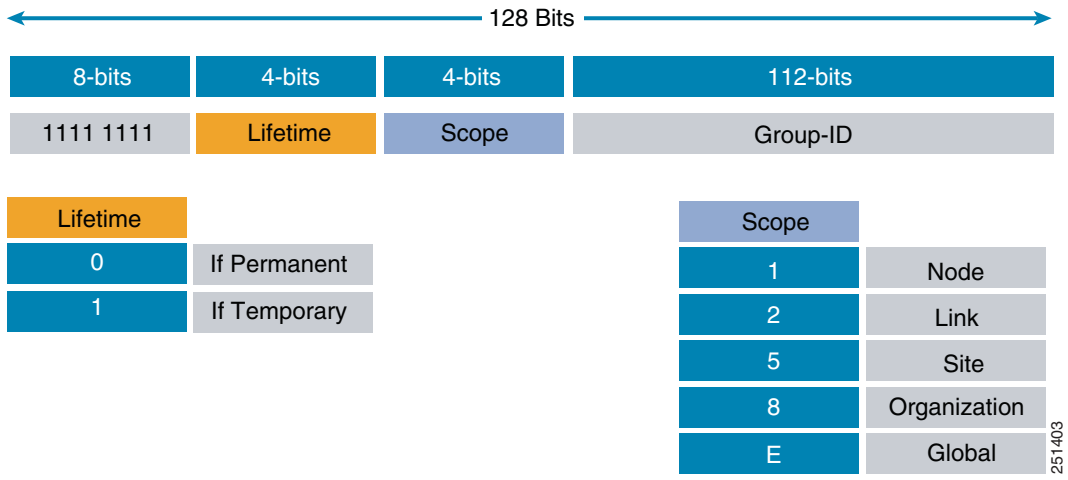
This address would generally be represented in shorthand notation as:

FE80::987:65FF: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 (see Figure 2-7).

***Figure 2-7 Multicast Address Format***




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

**Note** A default gateway configuration is not required by IPv6 clients because routers are discovered using RSs and RAs.

Table 2-1 lists some well known multicast addresses.

***Table 2-1 Common Multicast Addresses***

| Address | Scope | Meaning |
|---|---|---|
| FF01::1 | Node-local | Same node |
| FF02::1 | Link-local | All nodes on a link |
| FF01::2 | Node-local | Same router |
| FF02::2 | Link-local | All routers on a link |
| FF05::2 | Site-local | All routers on the Internet |
| FF02::1:FFxx:xxxx | Link-local | Solicited node |

For more information on IPv6 multicast addresses, refer to the IANA documentation available at

http://www.iana.org/assignments/ipv6-multicast-addresses

# Address Assignment for IPv6 Devices

IPv6 provides the following mechanisms for assigning address to IPv6 devices:



## Manual Configuration

An IPv6 address can be configured statically by a human operator. This can be an appropriate method of assigning addresses for router interfaces and static network elements and resources. However, manual assignment is open to errors and operational overhead due to the 128-bit length and hexadecimal attributes of the addresses.

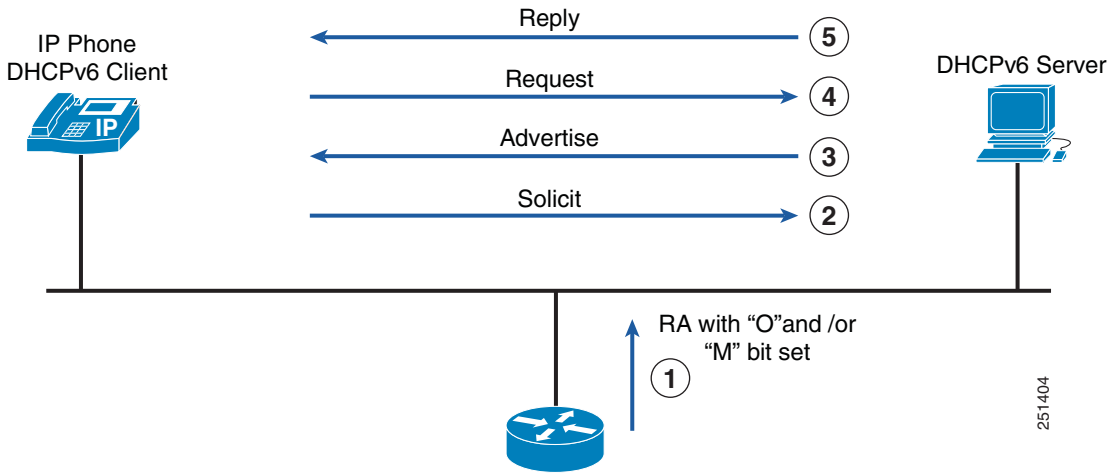
## IPv6 Stateless Address Auto-Configuration (RFC2462)

Stateless address auto-configuration (SLAAC) provides a convenient method to assign IP addresses to IPv6 nodes. This method does not require any human intervention from an IPv6 user. If you want to use IPv6 SLAAC on an IPv6 node, then it is important to connect that IPv6 node to a network with at least one IPv6 router. This router is configured by the network administrator and sends out Router Advertisement (RA) announcements onto the link. These announcements can allow the on-link connected IPv6 nodes to configure themselves with an IPv6 address and routing parameters, as specified in RFC2462, without further human intervention. With SLAAC, the node uses the IPv6 network prefix advertised in the link-local router's RAs and creates the IPv6 host ID by using the phone'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 wishes to receive configuration parameters, it will send out a request on the attached local network to detect available DHCPv6 servers. This is done through the Solicit and Advertise messages (see Figure 2-8). Well-known DHCPv6 multicast addresses are used for this process. Next, the DHCPv6 client will Request parameters from an available server, which will respond with the requested information in a Reply message. Like DHCPv4, DHCPv6 uses an architectural concept of "options" to carry additional parameters and information within DHCPv6 messages.

*Figure 2-8 IPv6 DHCP operation*




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.

For details on Cisco IOS DHCP configuration, see Example Configuration for a Cisco IOS IPv6 DHCP Server, page 5-6.

## Stateless DHCP

Stateless DHCPv6 is a combination of Stateless Address Auto-Configuration and Dynamic Host Configuration Protocol for IPv6, and it is specified by RFC3736. When a router sends an RA with the O bit set but does not set the M bit, the client can use Stateless Address Auto-Configuration (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 keep track of 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 will also return "other" configuration information together with the addresses. This mechanism is known as Stateful DHCPv6 because the DHCPv6 server does keep track of the client address bindings.

# DNS for IPv6

Cisco 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 (see Table 2-2), 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 2-2 DNS Name and Address Resolution*

| Resolution of: | IPv4 | IPv6 |
|---|---|---|
| Host name to IP address | **A record:** www.abc.test. A 192.168.30.1 | **AAAA record:** www.abc.test AAAA 2001:db8:C18:1::2 |
| IP address to host name | **PTR record:** 1.30.168.192.in-addr.arpa. PTR www.abc.test. | **PTR record:** 2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.0.0.0.8.1.c.0.8.b.d.0.1.0.0.2.ip6.arpa PTR www.abc.test. |

CHAPTER 3

# IPv6 Support in Cisco Unified Communications Devices

**Revised: June 08, 2010; OL-19142-02**

This chapter provides an introduction to the new terminology that is used with IPv6 for Cisco Unified Communications as well as a summary of the Cisco Unified Communications devices that support IPv6.

## IPv4 and IPv6 Terminology and Icons

The development of IPv6 introduces new concepts for Unified Communications networks, in particular the concept of a device's IP addressing mode. Devices may now support IPv4 only, IPv6 only, or IPv4 and IPv6 addresses. This document uses the symbols (or icons) shown in Figure 3-1 to represent the IP addressing mode capabilities of devices.

***Figure 3-1 Symbols Used to Represent IP Addressing Modes***


IPv4 Only
This device communicates with and understands IPv4 addresses only.


IPv6 Only
This device communicates with and understands IPv6 addresses only.


Dual Stack (IPv4 and IPv6)
This device can communicate with and understand both IPv4 and IPv6 addresses.


IPv6 Aware
This device communicates with IPv4 addresses, but it can receive and understand IPv6 addresses embedded in application protocol data units (PDUs). Typically this format is used by applications that use IPv4 to transport IPv6 information (for example, Cisco Unified Provisioning Manager).

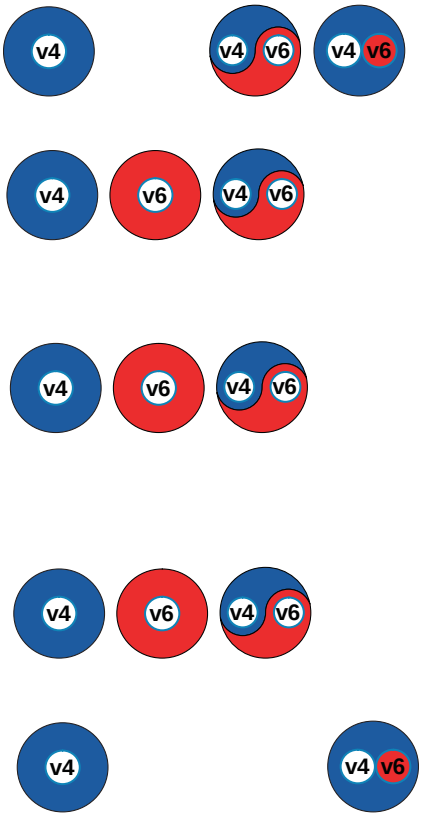
251405

**Note** For dual-stack (IPv4 and IPv6) Unified Communications devices such as Cisco IP Phones, 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.

# Support for IPv6 in Cisco Unified Communications Products

Figure 3-2 lists the Cisco Unified Communications products that support IPv6.

***Figure 3-2 Addressing Modes Supported by Cisco Unified Communications Products***




**Cisco Unified Communications Manager 7.1 and later releases:**

- All Cisco Media Convergence Server (MCS) platforms

**Cisco IP Phones:**

- Third generation Cisco IP Phones running SCCP only :

  Cisco 7906G, Cisco 7911G, Cisco 7931G, Cisco 7941G, Cisco 7941GE
  Cisco 7942G, Cisco 7945G, Cisco 7961G, Cisco 7961GE, Cisco 7962G
  Cisco 7965G, Cisco 7970G, Cisco 7971G-GE, Cisco 7975G

**Gateways**

- SIP gateways (Cisco ISR 2800 and 3800 Series; Cisco AS5400)
- Cisco VG224 SCCP Analogue Gateway
- SCCP FXS ports on Cisco ISR 2800 and 3800 Series Routers
- Cisco IOS MTPs for IPv4-to-IPv6 RTP media conversion

**Cisco Unified CM SIP Trunks**

**Applications**

- Cisco Unified CM CTI (IPv6 aware)
- Cisco Unified CM AXL/SOAP interface (IPv6 aware)
- Cisco Unified CM SNMP (IPv6 aware)

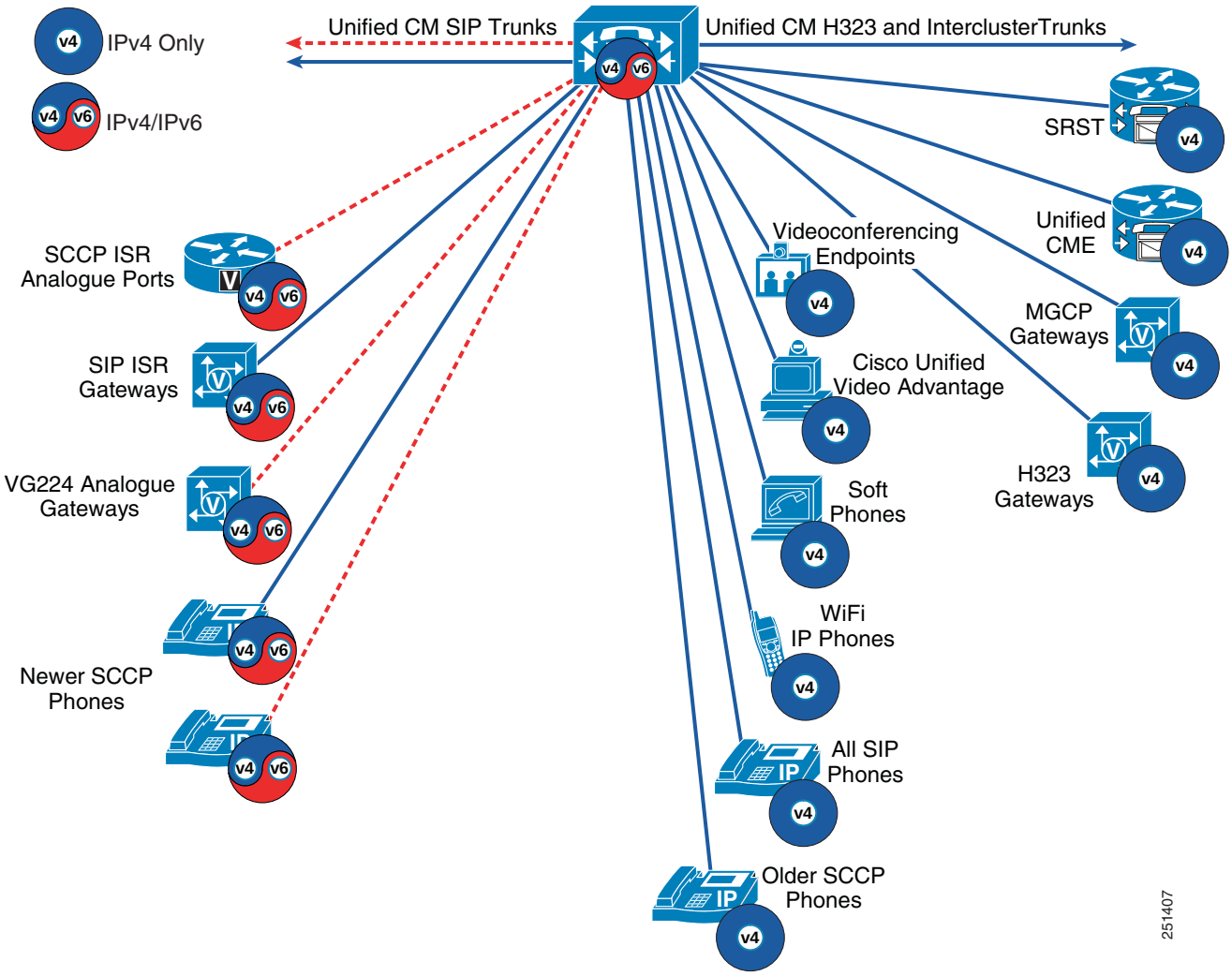
251406

Only the devices and applications listed in Figure 3-2 support IPv6. All other Cisco Unified Communications devices and applications support IPv4. For Unified Communications implementations, Cisco recommends that you configure all IPv6 devices and applications in dual-stack (IPv6 and IPv4) mode or IPv4-only mode. This ensures interoperability with existing IPv4-only devices and applications. Cisco IP Phones can be configured as IPv6 only, but this configuration is not recommended in production environments.

# Addressing Modes Supported by Cisco Unified Communications Devices

Figure 3-3 illustrates the addressing modes available for Cisco Unified Communications devices that support IPv6. For signaling with dual-stack (IPv4 and IPv6) devices, each device can support either IPv4 or IPv6. For media with dual-stack devices, each device can support IPv4 only, IPv6 only, or IPv4 and IPv6.

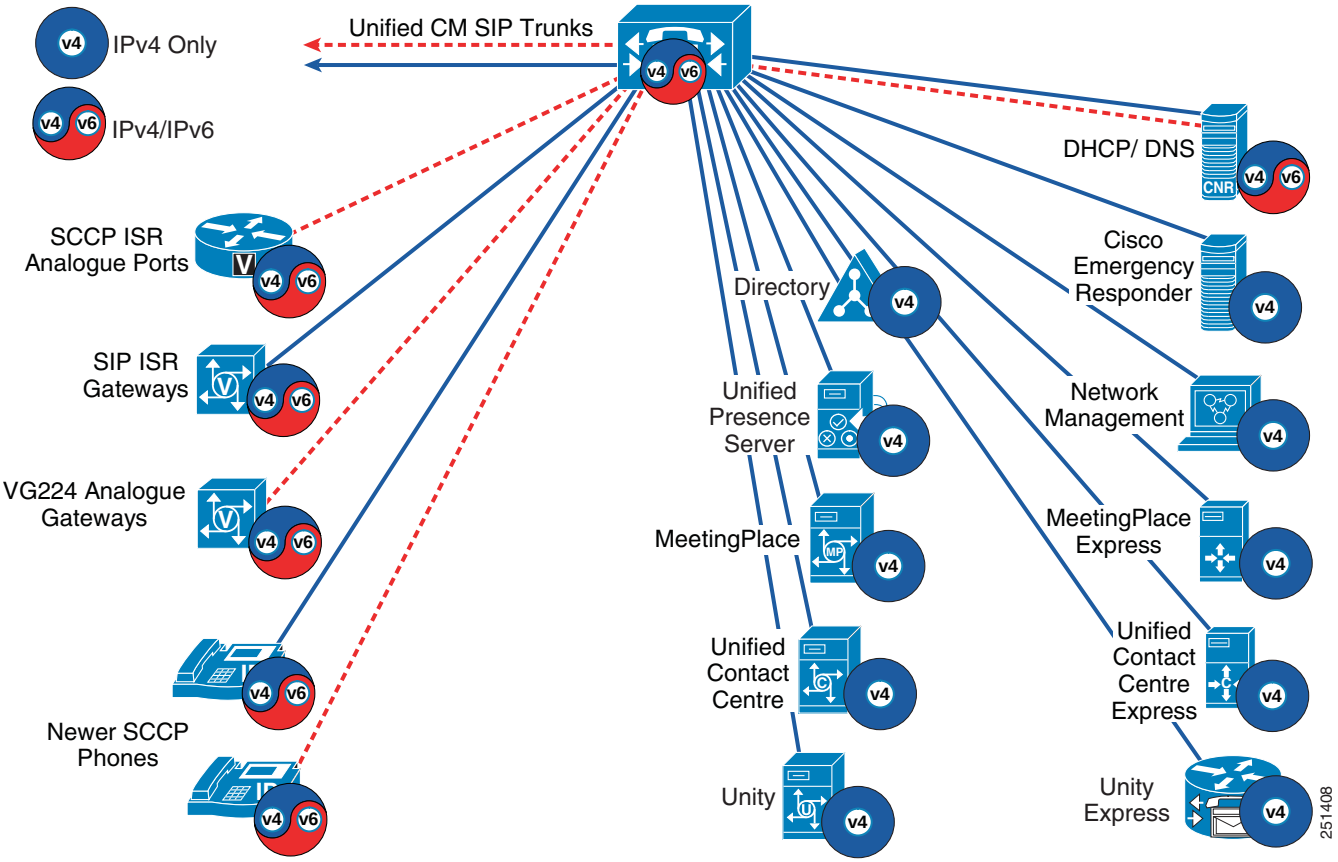
***Figure 3-3 Addressing Modes for Cisco Unified Communications IPv6 Devices***



# Addressing Modes Supported by Cisco Unified Communications Applications

Figure 3-4 illustrates the addressing modes available for Cisco Unified Communications applications that support IPv6.

***Figure 3-4 Addressing Modes for Cisco Unified Communications IPv6 Applications***



# IPv6 Addressing in Cisco Unified Communications Products

The previous sections discussed the various addressing modes supported by Cisco Unified Communications devices. This section describes how many IPv6 addresses each of these devices 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:
  - One IPv6 unique local address (for example, FD00:AAAA:BBBB:CCCC:0987:65FF:FE01:2345)
  - Or one IPv6 global address (for example, 2001:0DB8:BBBB:CCCC:0987:65FF:FE01:2345)
- One IPv4 address

All IPv6 devices must have a link local address.

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** 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.

## 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 and/or unique local addresses. The IP phone can use only one of these global or unique local IPv6 addresses to register to Cisco Unified Communications Manager. Once registered, 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 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 DHCPv6 to assign an address.
3. If neither a manually configured address nor a DHCPv6 address is available, but auto-configuration (SLAAC) is enabled for the phone (in Cisco Unified Communications Manager, the SLAAC default = On), then the phone will use SLAAC to create an IPv6 address. With SLAAC, the phone uses the IPv6 network prefix advertised in the link local router's Router Advertisements (RAs) and creates the IPv6 host ID by using the phone's MAC address and the EUI-64 format for host IDs. If SLAAC is used and DHCP is disabled, a TFTP server address must be configured manually to enable the phone to register with Cisco Unified Communications Manager).

## 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, 2001:0DB8:BBBB:CCCC:0987:65FF:FE01:2345)
- Multiple IPv4 addresses

Cisco IOS media termination points (MTPs) are associated with the router's interface through the **sccp local** <*interface*> command, and they inherit the IPv4 and IPv6 addresses of the interface.

# Cisco Unified Communications Configuration Parameters and Features for IPv6

This section introduces the following new features and configuration parameters in Cisco Unified Communications Manager (Unified CM) to support IPv6:

- Common device configuration for phones and trunks
  - IP addressing mode
  - IP addressing mode preference for signaling
  - Allow auto-configuration for phones
- The new role of the MTP in IPv6-enabled Unified CM clusters
- Alternative Network Address Types (ANAT) for SIP trunks
- New enterprise parameters
- MTP selection

With Unified CM 8.0, IPv6 can be enabled and configured cluster-wide and at the device level, thus allowing Unified Communications IPv6 devices to be configured to use IPv6 for signaling and/or media. The features listed above are discussed in some detail here and in greater depth in later chapters.

# Common Device Configuration

Cisco Unified CM supports two IPv6 devices, IP phones and SIP trunks (to gateways or other Unified CM clusters). Rather than add IPv6 configuration parameters to specific trunks and phones, a Unified CM configuration template contains IPv6-specific configuration parameters for phones and SIP trunks. This section describes that template, which is known as the *common device configuration*.

The common device configuration profile (**Device** -> **Device Settings** -> **Common Device Configuration**) contains the following IPv6 configuration information:

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

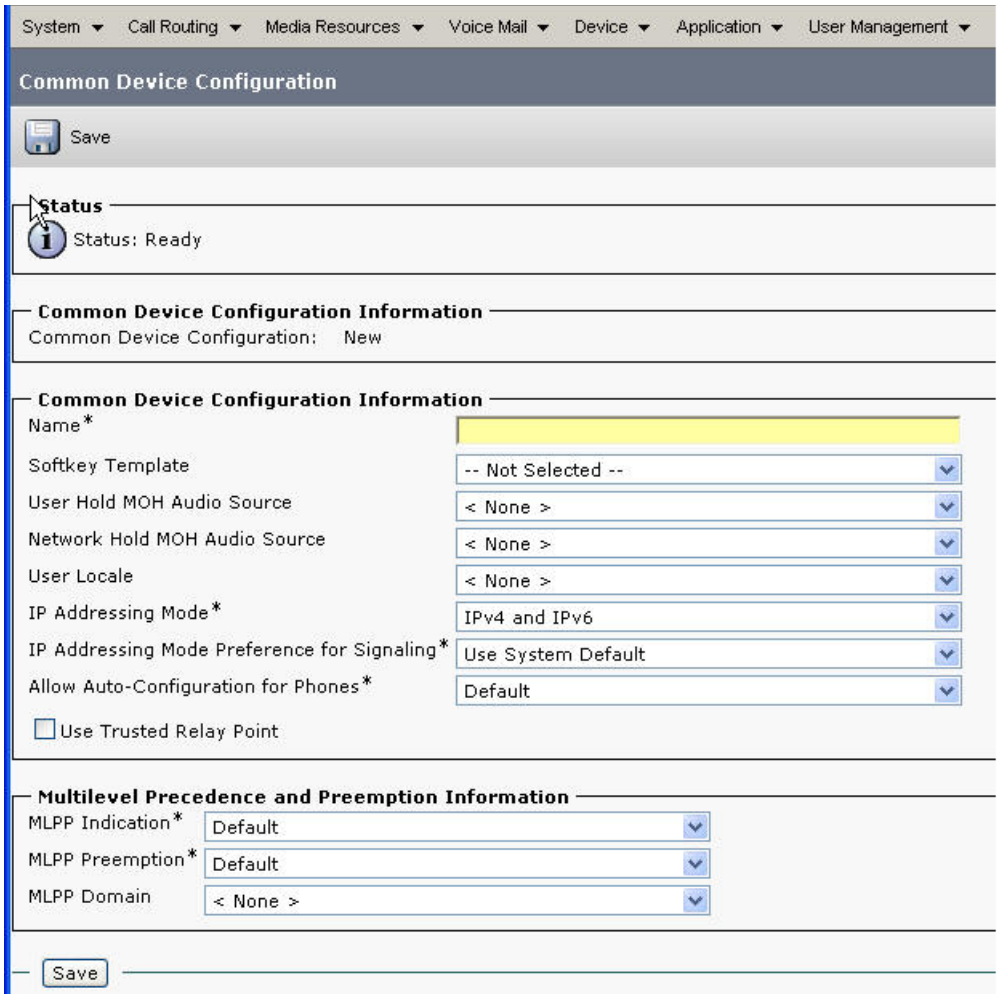
Multiple common device configuration profiles can be created and associated with devices such IP phones and SIP trunks. The following sections describe the configuration options for phones and SIP trunks.

### Default Common Device Configuration

There is no default common device configuration profile, and each device is initially associated with a <None> common device configuration (see Figure 3-5). If IPv6 is enabled in the Unified CM cluster with this <None> configuration, IPv6 devices adopt the following settings:

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

*Figure 3-5 Initial Common Device Configuration Settings*




## Common Device Configuration for IPv6 Phones

You can configure the common device configuration profile and assign it to the phones to apply one of the following IP addressing modes to the phones (see Figure 3-6):

- IPv4 Only

  In this addressing mode, the phone will acquire and use only one IPv4 address for all signaling and media. If the phone has acquired an IPv6 address previously, it will be released.

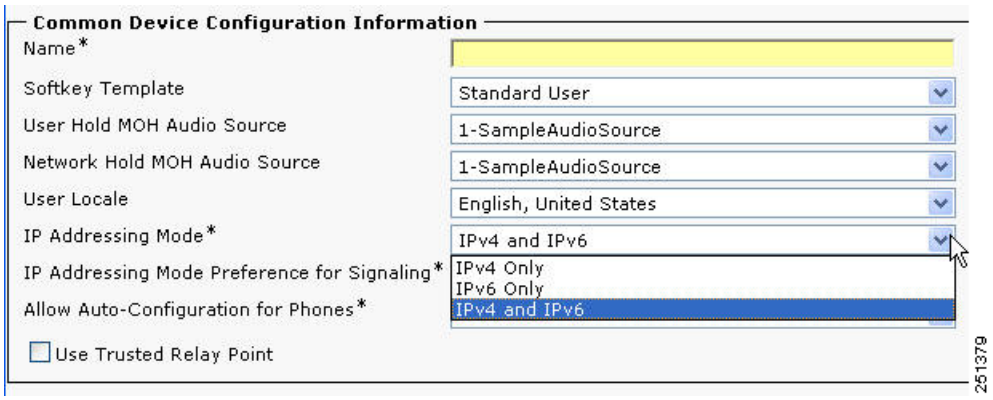
- IPv6 Only

  In this addressing mode, the phone will acquire and use only one IPv6 address for all signaling and media. If the phone has acquired an IPv4 address previously, it will be released.

- IPv4 and IPv6

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

*Figure 3-6 Setting the Phone IP Addressing Mode*




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

**Note** Cisco recommends **IPv4 and IPv6** as the setting for the phone IP addressing mode. **IPv6 Only** is not recommended for production environments.

## IP Addressing Modes for Media Streams Between Devices, and the New Role of the MTP for IPv6

As described previously, you can configure IPv6 devices to support a single IPv4 address, a single IPv6 address, or both an IPv4 address and an IPv6 address (also known as dual stack configuration). Furthermore, devices that do support both an IPv4 address and an IPv6 address can choose to use either their IPv4 addresses or their IPv6 addresses to transport RTP voice streams between the devices. The selection of IPv4 or IPv6 for media is determined by the Unified CM cluster-wide setting of **IP Addressing Mode Preference for Media**. (For details, see Cluster-Wide Configuration (Enterprise Parameters), page 3-13.)

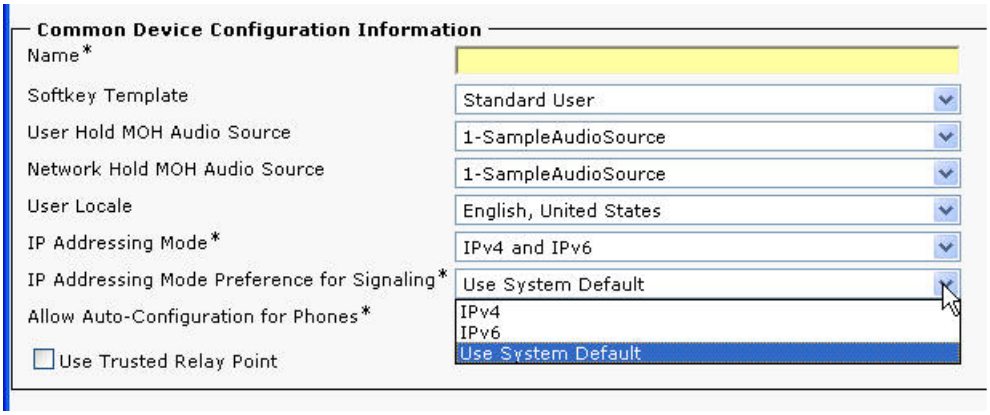
For two devices (such as phones) that support mismatched addressing modes, an IP addressing version incompatibility exists when a device with an IPv4 address wants to establish a RTP voice stream with a device with an IPv6 address. To resolve this IP addressing incompatibility for media, Unified CM dynamically inserts a media termination point (MTP) to convert the media stream from IPv4 to IPv6, and vice versa. For more information on how and when MTPs are used for IPv6 calls, see the chapter on Media Resources and Music on Hold, page 8-1.

### IP Addressing Mode Preference for Signaling for Phones

The phone IP Addressing Mode Preference for Signaling has three settings (see Figure 3-7):

- IPv4 — If the phone has an IPv4 address, it will use that address for call control signaling to Unified CM.
- IPv6 — If the phone has an IPv6 address, it will use that address for call control signaling to Unified CM.
- Use System Default — The phone will use the configured cluster-wide enterprise parameter value for its IP Addressing Mode for Signaling, if it has an address of that type.

*Figure 3-7 Setting the Phone IP Addressing Preference 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 only or IPv4 and IPv6, it will adopt the cluster-wide setting for IP Addressing Mode for Signaling, but all IPv4 phones will ignore this setting.

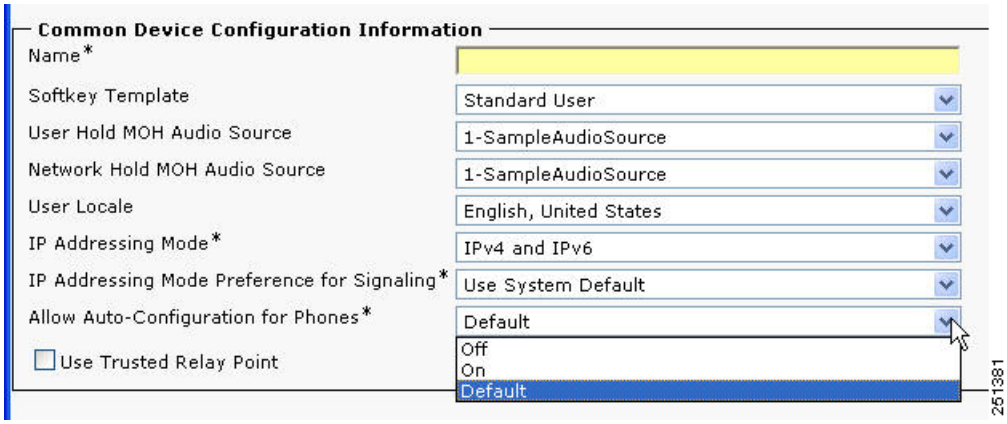
### Allow Auto-Configuration for Phones

The parameter to Allow Auto-Configuration for Phones has three settings (see Figure 3-8):

- On — The Phone is allowed to use Stateless Auto Address Configuration (SLAAC) to acquire an IPv6 address. Whether or not the phone will use SLAAC depends on the link local router's configuration of the O bit and M bit in Router Advertisements (RAs):
  - If the O bit is set in the router's RAs, the phone will use SLAAC to acquire its IP address and will use the DHCP server to acquire other information (such as the TFTP server address and DNS server address). This is known as stateless DHCP.
  - If the M bit is set in the router's RAs, the phone will not use SLAAC but will use the DHCP server to acquire its IP address and other information. This is known as stateful DHCP.
  - If neither the M bit nor the O bit is set, the phone will use SLAAC to acquire an IP address but will not use DHCP for other information. The phone will also require a TFTP server address to download its configuration file and register to Unified CM. This TFTP server address can be configured manually though the phone's user interface (UI).
- Off — The phone will 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 — The phone will use the cluster-wide enterprise parameter configuration value for **Allow Auto-Configuration for Phones**.

*Figure 3-8 Setting the Parameter to Allow Auto-Configuration for Phones*




If IPv6 is enabled in the Unified CM cluster, the phone's default setting for Allow Auto-Configuration for Phones setting is **Default**. If the IP phone supports either IPv6 only or IPv4 and IPv6, it will adopt the cluster-wide setting for Allow Auto-Configuration for Phones, but all IPv4 phones will ignore this setting.

## Common Device Profile Configuration for Unified CM SIP Trunks

You can apply SIP trunk configuration settings either through the Common Device Configuration profile that you create and assign to the SIP trunk (IP Addressing Mode and IP Addressing Mode Preference for Signaling) or through the SIP profile configuration you assign to the SIP trunk (Enable ANAT).

With IPv6 enabled and with an IPv6 and IPv4 address 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 and IPv6 address.

### IP Addressing Mode

The SIP trunk IP addressing mode has three settings:

- IPv4 only — The SIP trunk will use the Unified CM IPv4 address for signaling and either an MTP IPv4 address or a phone IPv4 address for media.
- IPv6 only — The SIP trunk will use the IPv6 address for signaling and either an MTP or phone IPv6 address for media.
- IPv4 and IPv6 — 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.

For more information on these SIP trunk IP addressing modes, see SIP Trunks Using Delayed Offer, page 7-14.

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.

Cisco recommends setting the IP addressing mode for IPv6 SIP trunks to **IPv4 and IPv6**. The **IPv6 Only** setting is not recommended and should not be used in production environments.

#### IP Addressing Mode Preference for Signaling

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

- IPv4 — The SIP trunk will use the Unified CM IPv4 address as its source address for SIP signaling.
- IPv6 — The SIP trunk will use the Unified CM IPv6 address as its source address for SIP signaling.
- Use System Default — The SIP trunk will use 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

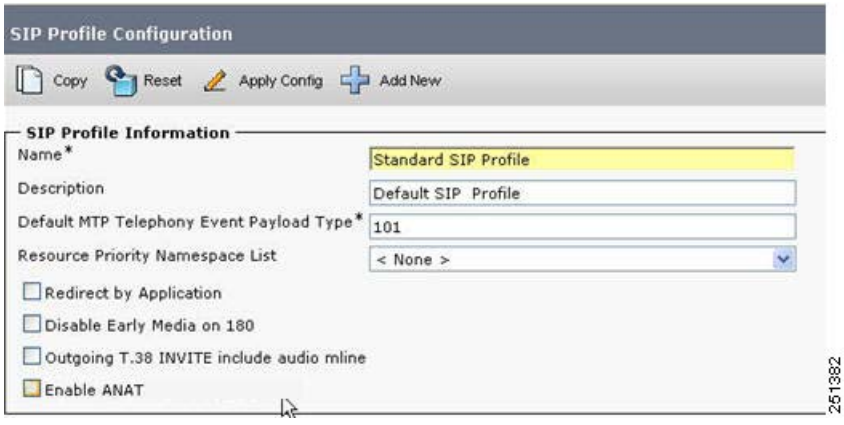
The parameter to Allow Auto-Configuration for Phones is not used by SIP trunks.

### Alternative Network Address Types (ANAT)

Alternative Network Address Types (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.

Cisco supports ANAT over dual-stack (IPv4 and IPv4) 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 (see Figure 3-9). ANAT can be used with both Early Offer and Delayed Offer calls.

*Figure 3-9 SIP Trunk Profile Configuration*




For more information on ANAT, see Alternative Network Address Types (ANAT), page 7-10.

**Note** Enable ANAT only on SIP trunks with an IP addressing mode setting of **IPv4 and IPv6**.

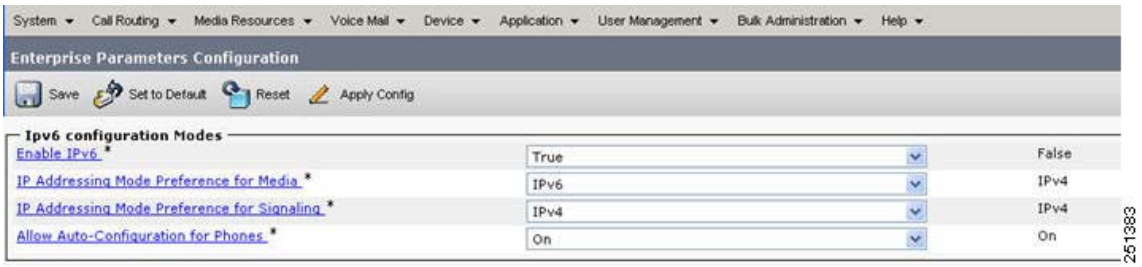
# Cluster-Wide Configuration (Enterprise Parameters)

Before configuring the cluster-wide parameters in Unified CM, you must 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 (see Figure 3-10):

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

***Figure 3-10 Cluster-Wide IPv6 Configuration Modes***




### Enable IPv6

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

### IP Addressing Mode Preference for Media

IP Addressing Mode Preference for Media has two setting options:

- IPv4 (default)
- IPv6

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 serves two purposes:

- The IP Addressing Mode Preference for Media is used to select which IP addressing version will be used for media when a call is made between two dual-stack devices.
- The IP Addressing Mode Preference for Media is also 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 vice versa.

Typically both devices will 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 vice versa) 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 will be 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 will be 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 will be used.
- If no MTPs are available, the call will fail.

MTP resource allocation is discussed in detail in the chapter on Media Resources and Music on Hold, page 8-1.

#### 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)
- IPv6

#### Allow Auto-Configuration for Phones

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

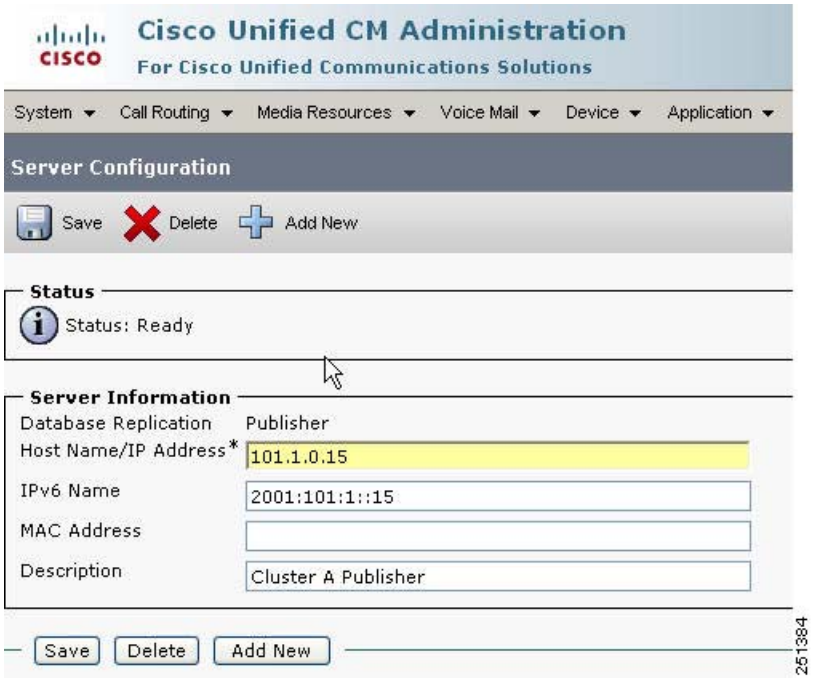
The parameter to Allow Auto-Configuration for Phones has two setting options:

- On (default)
- Off

# IPv6 Address Configuration for Unified CM

Once you have configured an IPv6 address for the Unified CM server (see Configuring IPv6 in Cisco Unified CM, page A-1), you must also configure this address in the Unified CM Administration graphical user interface (see Figure 3-11). This IPv6 address is used in the device configuration files stored on the cluster's TFTP server(s). 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 3-11 IPv6 Address Configuration for Unified CM***



CHAPTER 4

# Unified Communications Deployment Models for IPv6

**Revised: June 08, 2010; OL-19142-02**

This chapter describes the deployment models you can use with IPv6 in Cisco Unified Communications networks. Cisco Unified Communications Manager (Unified CM) 8.0 supports the following deployment models:

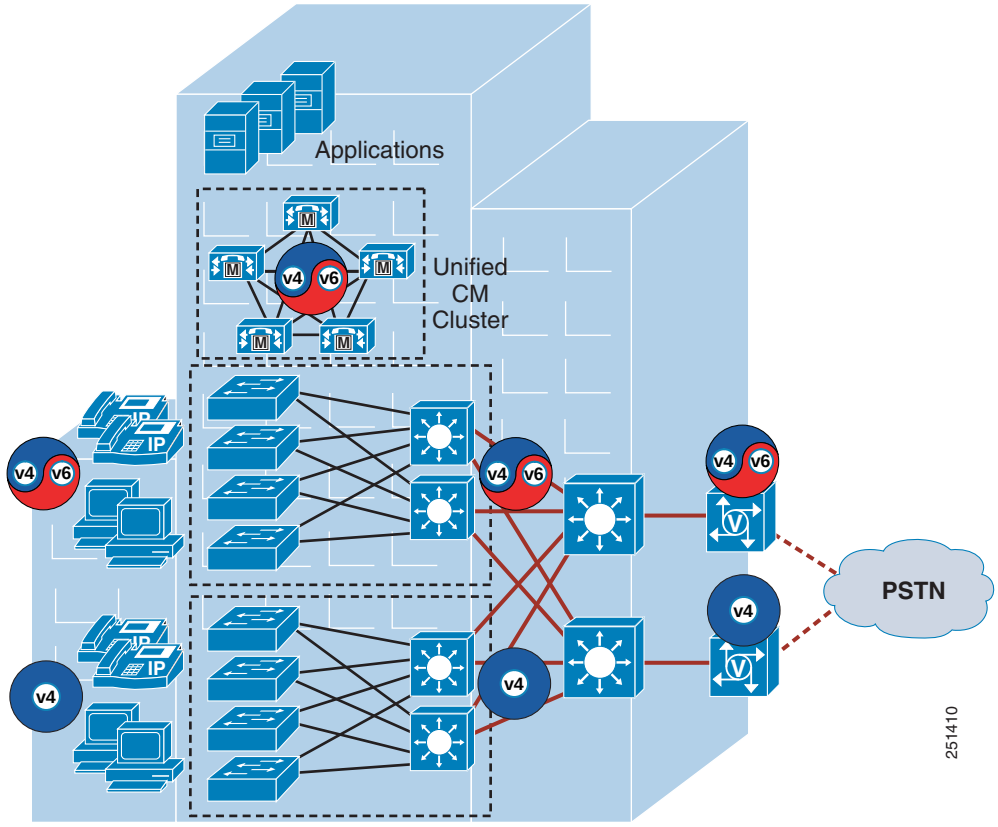
- Single-site deployments
- Multi-site WAN deployments with distributed call processing
- Multi-site deployments with centralized call processing and Survivable Remote Site Telephony (SRST)

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

## Single-Site Deployments

The single-site model for Cisco Unified Communications 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 traffic within the site. (See Figure 4-1.) In this model, calls beyond the LAN or MAN use the public switched telephone network (PSTN).

*Figure 4-1 Single-Site IPv6 Deployment*




The characteristics and benefits of the IPv6 single-site model are the same as those for IPv4 single-site deployments, as described in the *Cisco Unified Communications Solution Reference Network Design (SRND)*, available at http://www.cisco.com/go/ucsrnd. However, the IPv6 single-site model includes the additional IPv6 and dual-stack product capabilities and features discussed throughout this document.

# 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 (Recommended)
- IPv6 only (Not recommended for production environments)

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 PSTN gateways can be deployed in a single-site deployment. If only one gateway is deployed, a Unified CM SIP trunk and Cisco IOS SIP gateway should be used. Both the Unified CM SIP trunk and Cisco IOS SIP gateway should be configured as follows:

- Dual stack (IPv4 and IPv6)
- With ANAT enabled
- To use IPv6 for signaling
- To prefer IPv6 over IPv4 for media

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

- SIP Early Offer (**MTP required** checked and used for every call.)
- SIP Delayed Offer (**MTP Required** unchecked, although MTPs may be inserted dynamically for some calls for conversions between IPv4 and IPv6 addresses.)

If a single dual-stack gateway is used and the cluster-wide preference for media is set to IPv6, an MTP will be used for all calls to IPv4-only devices to convert from IPv4 to IPv6. 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 a dual-stack SIP gateway using SIP Delayed Offer as described above, and the other as a standard IPv4-only gateway. Calling search spaces and partitions can then be used to direct PSTN calls from IPv4-only and dual-stack devices to their respective gateways.

For specific device configuration options and preferences, refer to the chapters on Trunks, page 7-1, and Unified Communications Endpoints, page 15-1.

# The Campus LAN

If the campus LAN uses Layer 2 switching only, Multicast Listener Discovery (MLD) should be enabled, 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.

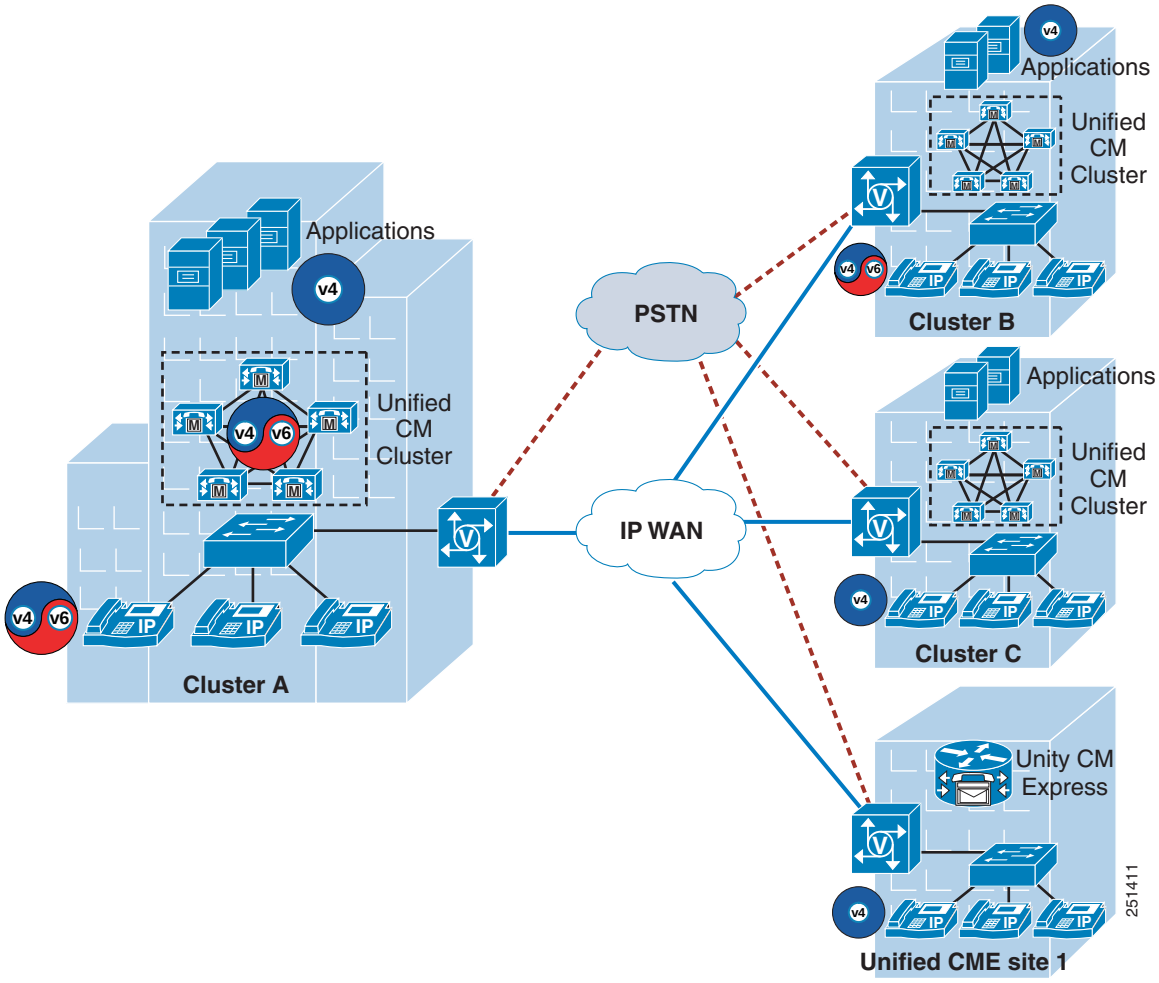
If the campus LAN also includes Layer 3 routing devices, these devices should be configured to support dual-stack (IPv4 and IPv6) routing.

**Note** If a single PSTN gateway (as described above) 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 dual-stack 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. (See Figure 4-2.)

***Figure 4-2 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)
  - A standard (IPv4 only) Cisco Unified Communications Manager (Unified CM)
  - A 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 dual-stack (IPv4 and IPv6))

For dual-stack (IPv4 and IPv6) sites, IPv6 devices should be configured as dual stack, with a preference of IPv6 for signaling and media. This configuration maximizes the amount of IPv6 traffic and minimizes 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 Unified Communications Solution Reference Network Design (SRND)*, available at http://www.cisco.com/go/ucsrnd. However, the IPv6 multi-site model includes the additional IPv6 and dual-stack product capabilities and features discussed in this document.

# Best Practices for IPv6 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-enabled SIP intercluster trunks to connect to other IPv6 Unified CM clusters. However, for intercluster trunk connections to IPv4-only Unified CM clusters, IPv6 intercluster trunks should not be used.

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

The Unified CM SIP intercluster trunks should be configured as follows:

- Dual stack (IPv4 and IPv6)
- With ANAT enabled
- To use IPv6 for signaling
- To prefer IPv6 over IPv4 for media (by configuring the cluster-wide addressing mode preference for media to IPv6)

The Unified CM SIP intercluster trunk can be configured to use either of the following:

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

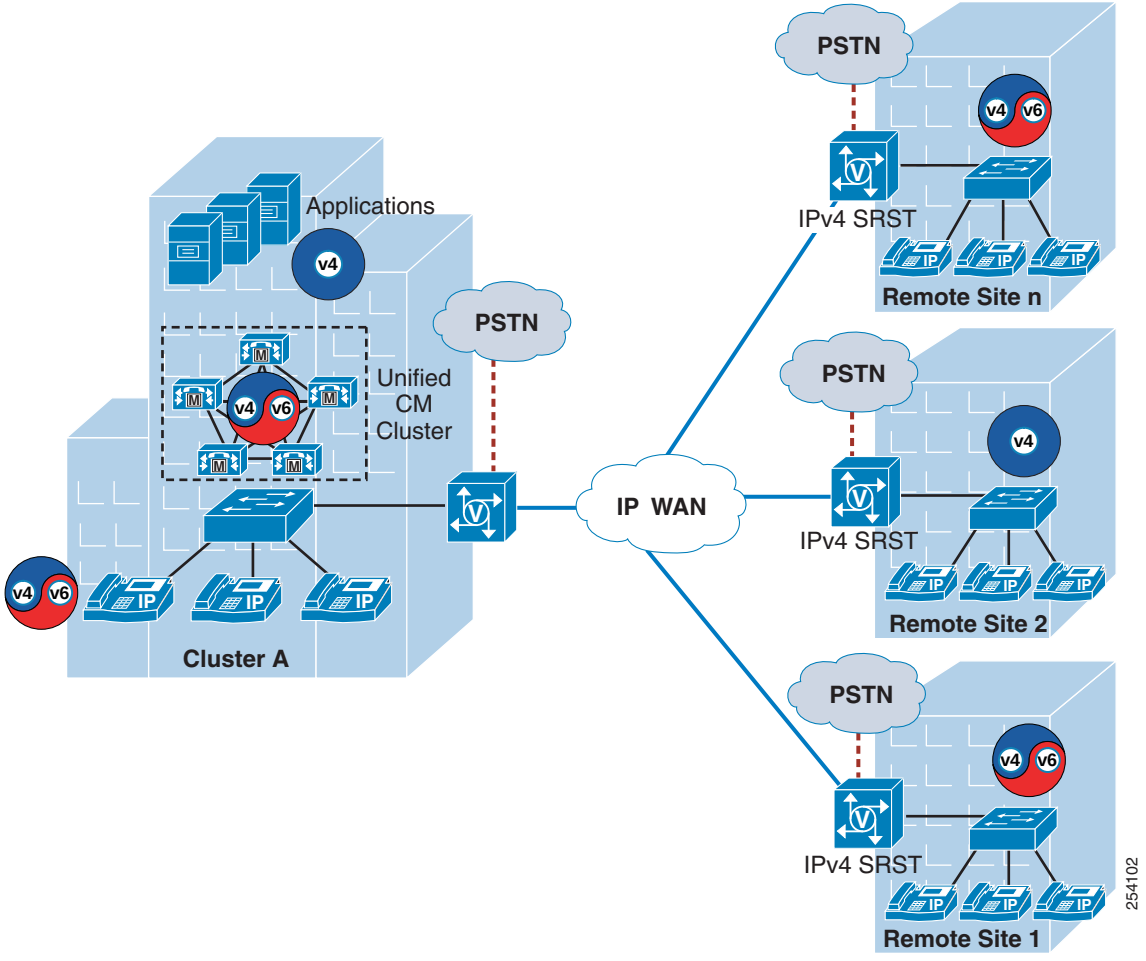
For specific device configuration options and preferences, refer to the chapters on Trunks, page 7-1, and Unified Communications Endpoints, page 15-1.

# Multi-Site Deployments with Centralized Call Processing and Survivable Remote Site Telephony (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. Figure 4-3 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.

*Figure 4-3 Multi-Site Deployment with Centralized Call Processing and SRST*



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-stack or IPv4 only. For dual-stack (IPv4 and IPv6) sites, IPv6 devices should be configured as dual-stack with a preference of IPv6 for signaling and media. This configuration maximizes the amount of IPv6 traffic and minimizes the use of 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 those for IPv4 multi-site centralized call processing deployments, as described in the *Cisco Unified Communications 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 and dual-stack product capabilities and features discussed in this document.

## Best Practices for IPv6 Multi-Site Deployments with Centralized Call Processing and Survivable Remote Site Telephony (SRST)

IPv6 multi-site deployments with centralized call processing can contain sites with a mixture of 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.

IPv6-capable phones can be configured as:

- IPv4 only
- IPv4 and IPv6 (Recommended)
- IPv6 only (Not recommended for production environments)

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

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

SRST routers at remote sites support IPv4 only in SRST mode. Dual-stack (IPv4 and IPv6) phones will revert to IPv4-only when in SRST mode and revert back to dual-stack mode when the connection to the Unified CM cluster is restored. IPv6-only phones do not support SRST and are not recommended for deployment at remote sites in production environments.

# 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. For more information on call admission control, refer to the *Cisco Unified Communications Solution Reference Network Design (SRND)*, available at http://www.cisco.com/go/ucsrnd.

# Intra-Cluster Communications

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

# Clustering Over the WAN

Clustering over the WAN with dual-stack Unified CM clusters has not been tested by Cisco Systems and is not currently supported.

# Call Detail Records (CDR) and Call Management Records (CMR)

Call detail records and call management records, 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.

CHAPTER 5

# Network Infrastructure

**Revised: June 08, 2010; OL-19142-02**

The requirements of the network infrastructure needed to build an IPv6 Unified Communications system in an enterprise environment are very similar to those for an IPv4 Unified Communications 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.

This chapter discusses recommendations specific to IPv6 for Unified Communications network infrastructures. For other guidance on standard network infrastructure features required in IPv4 Unified Communications networks, refer to the *Cisco Unified Communications Solution Reference Network Design (SRND)*, available at http://www.cisco.com/go/ucsrnd.

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 want to receive the data.
- Layer 3 routed networks require a mechanism to transport IPv6 traffic. Dual-stack (IPv4 and IPv6) routing is recommended, although a variety of 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 dual-stack 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 Unified Communications campus networks, refer to the *Cisco Unified Communications Solution Reference Network Design (SRND)*, available at http://www.cisco.com/go/ucsrnd.

## General IPv6 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*

  http://www.cisco.com/en/US/docs/solutions/Enterprise/Campus/CampIPv6.html
- *Deploying IPv6 in Branch Networks*

  http://www.cisco.com/en/US/docs/solutions/Enterprise/Branch/BrchIPv6.html

## IPv6 Design Guidance for Unified Communications Campus Networks

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

### MLD and MLD Snooping in Switched Layer 2 IPv6 Campus Networks

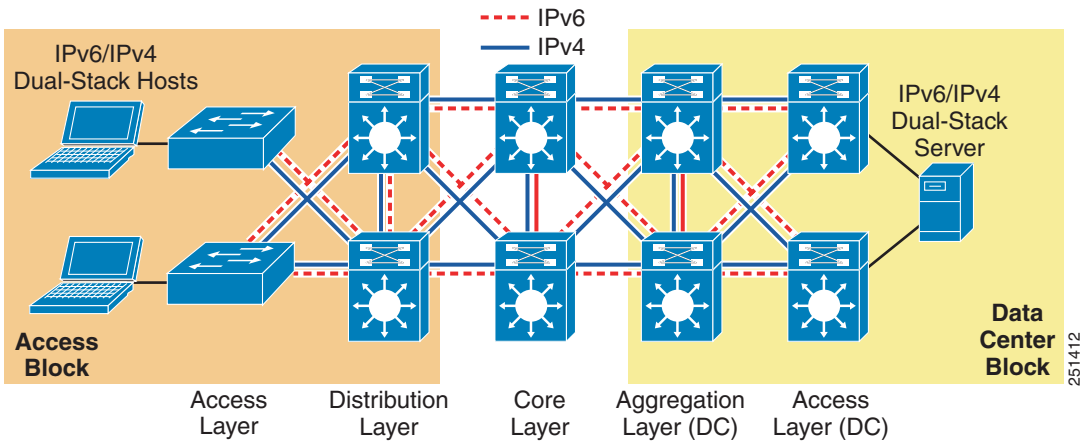
IPv6 multicast routers use Multicast Listener Discovery (MLD) protocol to discover the presence of multicast listeners (nodes wishing to receive IPv6 multicast packets) on its directly attached links and to discover which multicast packets are of interest to neighboring nodes.

MLD snooping is similar in concept 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

Cisco strongly recommends using dual-stack (IPv4 and IPv6) routing in Layer 3 campus IPv6 networks. (See Figure 5-1.) The Cisco Catalyst 6500 Series, 4500 E-Series, and 3750 Series Switches support Static, Routing Information Protocol next generation (RIPng), Enhanced Interior Gateway Routing Protocol (EIGRP), and Open Shortest Path First version 3 (OSPFv3) routing for IPv6.

*Figure 5-1 Dual-Stack Routing in a Campus Network*




# First-Hop Redundancy Protocols

In the campus hierarchical 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.

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 6000 Series Switches with Cisco IOS Release 12.2(33)SXI
  - Cisco Catalyst 4000 Series Switches with Cisco IOS Release 12.2(52)SG
  - Cisco Catalyst 3000 Series Switches with Cisco IOS Release 12.2(46)SE
- GLBP is supported on:
  - Cisco Catalyst 6000 Series Switches with Cisco IOS Release 12.2(33)SXI
  - Cisco Catalyst 4000 Series Switches with Cisco IOS Release 12.2(52)SG

  GLBP is not supported on the Cisco Catalyst 3000 Series Switches.

HSRP and GLBP first-hop redundancy protocols should be your first choice for high availability at the L2/L3 boundary because they have additional useful features such as interface tracking, router prioritization, and preemption. If your design does not permit the use of HSRP or GLBP, Neighbor Unreachability Detection (NUD) can be used as an alternative. Neighbor Discovery for IPv6 (RFC 2461) implements the use of Neighbor Unreachability Detection (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 by means of 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.

For additional information on configuring first-hop redundancy protocols, refer to the *Cisco IOS IPv6 Configuration Guide*, available at

http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/12_4t/ipv6_12_4t.html

# Network Services

As with IPv4 Unified Communications systems, the deployment of an IPv6 Unified Communications system requires the coordinated design of a well structured, highly available, and resilient network infrastructure as well as an integrated set of IPv6 network services including Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP), and Trivial File Transfer Protocol (TFTP). In general, the deployment guidelines for these network services are the same as for IPv4 Unified Communications 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 host names and network services to IPv6 addresses within a network or networks. DNS server(s) 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, thereby facilitating communications between network devices. Complete reliance on a single network service such as DNS can introduce an element of risk when a critical Unified Communications 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 can and will fail. For this reason, in networks requiring high availability, Cisco recommends that you do not rely on DNS name resolution for any communications between Cisco Unified Communications Manager (Unified CM) and the Unified Communications endpoints.

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

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

Cisco recommends the use of Cisco Network Registrar (CNR) as an IPv4 and IPv6 DNS server in your Unified Communications network. Other DNS server products may be used, but they have not been tested by Cisco Systems.

## 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 (namely, 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. Cisco recommends stateful DHCP host configuration for both IPv4 and IPv6 IP phones.

**Note** Unlike IPv4, which can use DHCP to inform a host of its default router, an IPv6 host uses Neighbor Discovery to find its local router(s).

As discussed previously, 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 Dual-Stack IP Phones

When the power is cycled on a dual-stack (IPv4 and 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

Cisco recommends the use of either a Cisco Network Registrar IPv4 and IPv6 DHCP server or a Cisco IOS IPv4 and IPv6 DHCP server in your Unified Communications network. Other DHCP server products may be used, but they have not been tested by Cisco systems.

## 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 **dhcp relay destination** 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:

**ipv6 dhcp relay destination** *ipv6-address* [*interface-type interface-number*]

## Cisco IOS DHCPv6 Server

Current Cisco IOS releases support Cisco IOS DHCPv6 server functionality, but not all platforms support IPv6 vendor-specific options. Cisco Catalyst platforms support the IPv6 DHCP server with vendor-specific options in Cisco IOS Release 12.2(46)SE. Cisco IOS Router platforms support IPv6 DHCP server functionality with support for vendor-specific options in Cisco IOS Release 12.4(22)T.

## Example 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 will be resolved via a DNS service query. The name resolution may result in several addresses being 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)

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 telephony 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 does not support NTP for IPv6; therefore, if Linux based NTP is used, IPv4 NTP should be used for Unified CM clock synchronization.

#### Cisco IOS and CatOS NTP Time Synchronization

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

# WAN Infrastructure

Proper WAN infrastructure design is extremely important for normal IP telephony 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 Unified Communications networks. For general guidance on designing WAN infrastructures for Unified Communications deployments, refer to the *Cisco Unified Communications Solution Reference Network Design (SRND)*, available at http://www.cisco.com/go/ucsrnd.

## General IPv6 Design Guidance

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

- Introduction to IPv6 in Cisco products

  http://www.cisco.com/en/US/products/ps6553/products_ios_technology_home.html

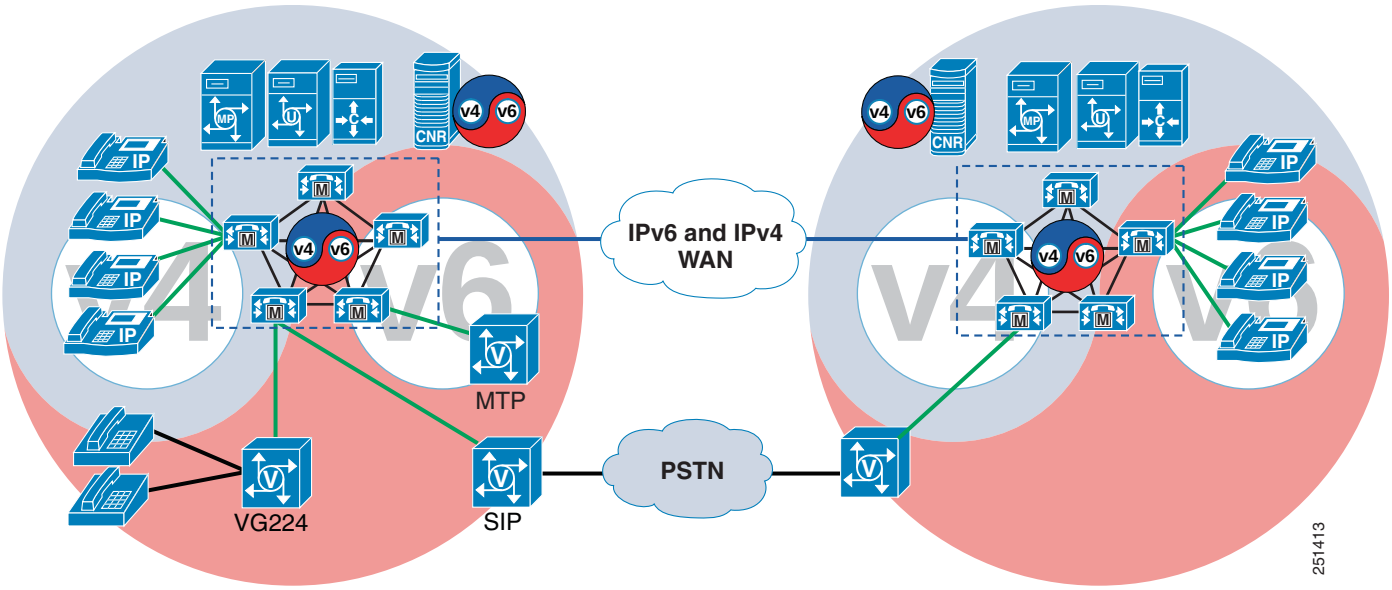
- *Deploying IPv6 in Branch Networks*

  http://www.cisco.com/application/pdf/en/us/guest/netsol/ns107/c649/ccmigration_09186a00807753ad.pdf

## 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. (See Figure 5-2.)

*Figure 5-2 Dual-Stack WAN Infrastructure*




The following deployment options are available for deploying IPv6 in a branch campus and across the WAN:

- 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

Cisco Unified CM 8.0 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 in keeping track of 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.

### Locations-Based Call-Counting Call Admission Control

Cisco Unified CM 8.0 also supports a type of locations-based, topology-unaware call admission control know 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.

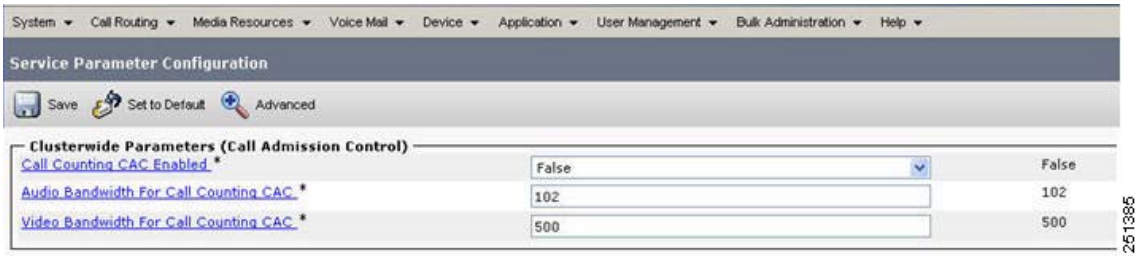
For call-counting call admission control, the following default values are used for Layer 3 voice and video bandwidth when calculating the amount of available bandwidth at a location:

- 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 (see Figure 5-3).

***Figure 5-3 Configuring Call Counting for Call Admission Control***




# IPv6 Bandwidth Provisioning

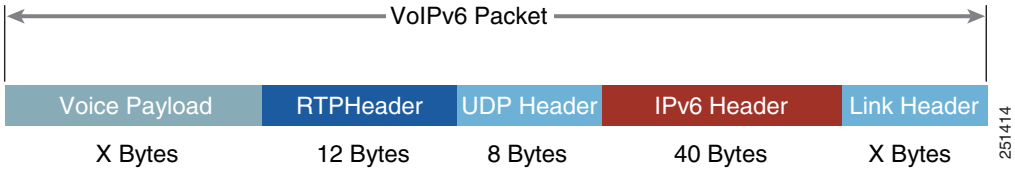
For general recommendations on bandwidth provisioning for Unified Communications traffic, refer to the bandwidth provisioning information in the *Cisco Unified Communications Solution Reference Network Design (SRND)*, available at http://www.cisco.com/go/ucsrnd. However, when provisioning for IPv6 voice bearer traffic, you must take into account the additional 20-byte overhead of the IPv6 header, as shown in the section on IPv6 Bandwidth Calculations, page 5-11.

**Note** Video traffic does not support IPv6. Video always uses IPv4. To determine the bandwidth requirements for video flows, refer to the bandwidth provisioning information in the *Cisco Unified Communications Solution Reference Network Design (SRND)*, available at http://www.cisco.com/go/ucsrnd.

# IPv6 Voice Bearer Traffic

As illustrated in Figure 5-4, 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.

***Figure 5-4 Typical VoIPv6 Packet***




# 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 = [(Packets per second) * (*X* bytes for voice payload + 60 bytes for RTP/UDP/IP headers + *Y* bytes for Layer 2 overhead) * 8 bits] / 1000

Layer 3 bandwidth in kbps = [(Packets per second) * (*X* bytes for voice payload + 60 bytes for RTP/UDP/IP headers) * 8 bits] / 1000

Packets per second = [1/(sampling rate in msec)] * 1000

Voice payload in bytes = [(codec bit rate in kbps) * (sampling rate in msec)] / 8

Table 5-1 details the Layer 3 bandwidth per VoIPv6 flow. Table 5-1 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. Table 5-1 does not include Layer 2 header overhead (see Table 5-2). The codec sampling rate can be adjusted through the Unified CM Service Parameters menu.

***Table 5-1 Layer 3 Bandwidth per VoIPv6 Flow***

| CODEC | Sampling Rate | Voice Payload in Bytes | Packets per Second | Bandwidth per Conversation |
|---|---|---|---|---|
| G.711 and G.722-64k | 20 ms | 160 | 50.0 | 88.0 kbps |
| G.711 and G.722-64k (SRTP) | 20 ms | 164 | 50.0 | 89.6 kbps |
| G.711 and G.722-64k | 30 ms | 240 | 33.3 | 79.2 kbps |
| G.711 and G.722-64k (SRTP) | 30 ms | 244 | 33.3 | 81.0 kbps |
| iLBC | 20 ms | 38 | 50.0 | 39.2 kbps |
| iLBC (SRTP) | 20 ms | 42 | 50.0 | 40.8 kbps |
| iLBC | 30 ms | 50 | 33.3 | 29.3 kbps |
| iLBC (SRTP) | 30 ms | 54 | 33.3 | 30.4 kbps |
| G.729A | 20 ms | 20 | 50.0 | 32.0 kbps |

*Table 5-1 Layer 3 Bandwidth per VoIPv6 Flow (continued)*

| CODEC | Sampling Rate | Voice Payload in Bytes | Packets per Second | Bandwidth per Conversation |
|---|---|---|---|---|
| G.729A (SRTP) | 20 ms | 24 | 50.0 | 33.6 kbps |
| G.729A | 30 ms | 30 | 33.3 | 24.0 kbps |
| G.729A (SRTP) | 30 ms | 34 | 33.3 | 25.0 kbps |

# 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. Table 5-2 lists the amount of bandwidth consumed by IPv6 voice traffic when the Layer 2 headers are included in the calculations.

*Table 5-2 Bandwidth Consumption with Layer 2 Headers Included*

| | Header Type and Size | | | | | | |
|---|---|---|---|---|---|---|---|
| CODEC type and packet rate (packets per second) | Ethernet 14 Bytes | PPP 6 Bytes | ATM 53-Byte Cells with a 48-Byte Payload | Frame Relay 4 Bytes | MLPPP 10 Bytes | MPLS 4 Bytes | WLAN 24 Bytes |
| G.711 and G.722-64k at 50.0 pps | 93.6 kbps | 90.4 kbps | 109.2 kbps | 89.6 kbps | 92 kbps | 89.6 kbps | 97.6 kbps |
| G.711 and G.722-64k (SRTP) at 50.0 pps | 95.2 kbps | 92 kbps | 110.8 kbps | 91.2 kbps | 93.6 kbps | 91.2 kbps | 99.2 kbps |
| G.711 and G.722-64k at 33.3 pps | 83.7 kbps | 81.5 kbps | 94.0 kbps | 80.1 kbps | 82.6 kbps | 80.1 kbps | 86.3 kbps |
| G.711 and G.722-64k (SRTP) at 33.3 pps | 84.7 kbps | 82.6 kbps | 95.1 kbps | 82.1 kbps | 83.7 kbps | 82.1 kbps | 87.4 kbps |
| iLBC at 50.0 pps | 44.8 kbps | 41.6 kbps | 60.4 kbps | 40.8 kbps | 43.2 kbps | 40.8 kbps | 48.8 kbps |
| iLBC (SRTP) at 50.0 pps | 46.4 kbps | 43.2 kbps | 62.0 kbps | 42.4 kbps | 44.8 kbps | 42.4 kbps | 50.4 kbps |
| iLBC at 33.3 pps | 33.0 kbps | 30.9 kbps | 43.5 kbps | 30.4 kbps | 32.0 kbps | 30.4 kbps | 35.7 kbps |
| iLBC (SRTP) at 33.3 pps | 34.1 kbps | 32.0 kbps | 44.5 kbps | 31.5 kbps | 33.1 kbps | 31.5 kbps | 36.8 kbps |
| G.729A at 50.0 pps | 37.6 kbps | 33.4 kbps | 53.2 kbps | 33.6 kbps | 36.0 kbps | 33.6 kbps | 41.6 kbps |
| G.729A (SRTP) at 50.0 pps | 39.2 kbps | 36.0 kbps | 54.8 kbps | 35.2 kbps | 37.6 kbps | 35.2 kbps | 43.2 kbps |
| G.729A at 33.3 pps | 27.7 kbps | 25.6 kbps | 38.1 kbps | 25.1 kbps | 26.7 kbps | 25.1 kbps | 30.4 kbps |
| G729A (SRTP) at 33.3 pps | 28.8 kbps | 26.7 kbps | 39.2 kbps | 26.1 kbps | 27.8 kbps | 26.1 kbps | 31.5 kbps |

## 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 and/or distributed call processing, you also need to consider bandwidth provisioning for inter-site signaling and/or intercluster trunk signaling traffic. For information on bandwidth provisioning for call control traffic over IPv4 trunks, refer to the *Cisco Unified Communications Solution Reference Network Design (SRND)*, available at 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. Cisco does not recommend the deployment of IPv6 in networks that use RSVP for call admission control.

## WLAN

IPv6 is not supported by any Cisco wireless Unified Communications devices such as the Cisco Wireless IP Phone 7920, 7921, or 7925. These devices support IPv4 only.

# Network Management

Cisco network management applications and products support IPv6 as follows:

- Cisco Unified Provisioning Manager is IPv6-aware
- The following products do *not* support IPv6-only devices:
  - Cisco Unified Operations Manager (IPv4 Only)
  - Cisco Unified Service Monitor (IPv4 Only)
  - Cisco Unified Service Statistics Manager (IPv4 Only)
  - Cisco Monitor Manager and Monitor Director (IPv4 Only)
  - Cisco netManager (IPv4 Only)

CHAPTER 6

# Gateways

**Revised: June 08, 2010; OL-19142-02**

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 Unified Communications Solution Reference Network Design (SRND)*, available at http://www.cisco.com/go/ucsrnd.

This section describes the Cisco voice gateways and interfaces that support IPv6. For gateway configuration examples, see:

- Configuring Cisco Integrated Services Routers, page B-1
- Configuring Cisco VG224 Analog Voice Gateway, page C-1
- Configuring Cisco IOS Gateways, page D-1

The following sections describe the IPv6-capable interfaces and features supported by various types of Cisco voice gateways. All other gateways not listed here support IPv4 only.

Connections that use H.323 and MGCP signaling protocols between Unified CM and the gateway support IPv4 only.

### Cisco 2800 and 3800 Series Integrated Services Routers

Cisco 2800 and 3800 Series Integrated Services Routers (ISRs) support the following features:

- TDM connections using SIP trunk signaling to Cisco Unified Communications Manager (Unified CM)
- FXS Analogue port connections using Skinny Client Control Protocol (SCCP) signaling to Unified CM
- Software and hardware media termination points (MTPs) for conversion between IPv4 and IPv6 using SCCP signaling to Unified CM

You can combine TDM, analogue port, and MTP functionality on a single Cisco Integrated Services Router (ISR) platform.

Cisco 2800 and 3800 Series Integrated Services Routers support the above IPv6 functionality in Cisco IOS Release 12.4(22)T.

The appendix on Configuring Cisco Integrated Services Routers, page B-1, contains Cisco ISR configurations for:

- An IPv6 SIP trunk (Note that Cisco TDM gateways support SIP Early Offer only.)
- SCCP-controlled IPv6 FXS ports
- Software MTPs

### Cisco AS5400 Series Universal Gateway

Cisco AS5400 Series Universal Gateways support high-density TDM connections using SIP trunk signaling to Unified CM. Cisco AS5400 Series Universal Gateways support this IPv6 functionality in Cisco IOS Release 12.4(22)T.

### Cisco VG224 Analog Voice Gateway

Cisco VG224 Analog Voice Gateways support up to 24 FXS ports using SCCP signaling to Unified CM. Cisco VG224 Analog Voice Gateways support this IPv6 functionality in Cisco IOS Release 12.4(22)T.

The appendix on Configuring Cisco VG224 Analog Voice Gateway, page C-1, contains a configuration example for the Cisco VG224 Analog Voice Gateway.

### Fax and Modem Support

Fax pass-through and fax relay over IPv6 are supported on SCCP-controlled FXS ports of Cisco Integrated Services Routers and VG224 Analog Voice Gateways.

Modem pass-through and modem relay over IPv6 are supported on SCCP-controlled FXS ports of Cisco Integrated Services Routers and VG224 Analog Voice Gateways.

CHAPTER 7

# Trunks

**Revised: June 08, 2010; OL-19142-02**

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 Unified Communications Solution Reference Network Design (SRND)*, available at http://www.cisco.com/go/ucsrnd.

There are several possible configurations for Unified CM SIP trunks. This chapter focuses on the following recommended configurations for IPv6 SIP trunks:

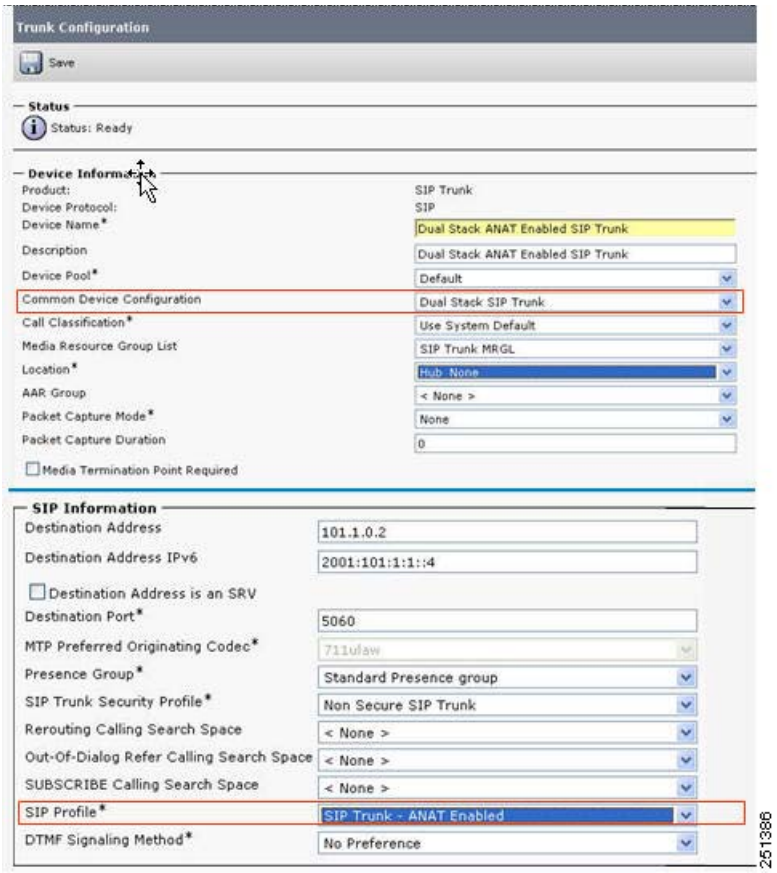
- Inbound and outbound SIP Early Offer trunk calls
- Inbound and outbound SIP Early Offer trunk calls with Alternative Network Address Types (ANAT) enabled
- Inbound and outbound SIP Delayed Offer trunk calls
- Inbound and outbound SIP Delayed Offer trunk calls with ANAT enabled

## Configuring IPv6 SIP Trunks

To configure SIP trunks to gateways and Unified CM SIP intercluster trunks, select **Devices** > **Trunks** > **SIP Trunk** in Unified CM Administration (see Figure 7-1).

The SIP trunk configuration settings discussed in this section get 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**).

*Figure 7-1 Trunk Configuration in Cisco 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 (see Figure 7-2):

- IPv4 only

  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 only

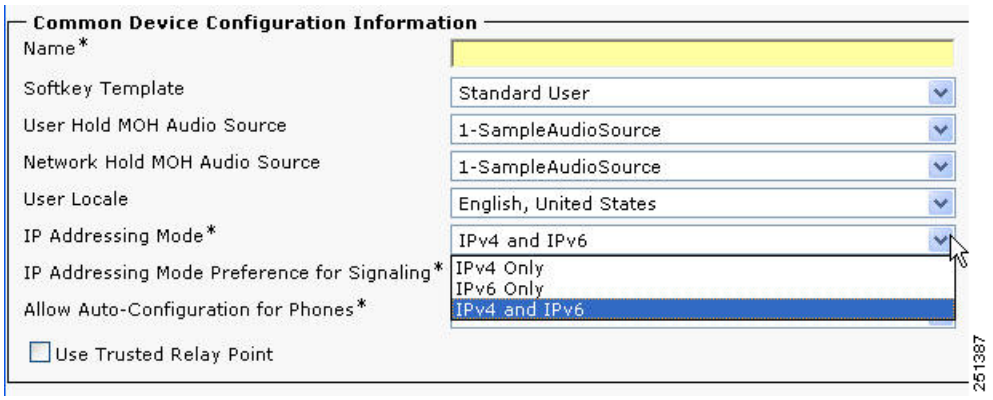
  In this mode, the SIP trunk uses the Unified CM IPv6 address for signaling and either an MTP or phone IPv6 address for media.

- IPv4 and IPv6

  In this mode, the SIP trunk uses either the Unified CM IPv4 address or the Unified CM IPv6 address for signaling, and either an MTP or phone IPv4 and/or IPv6 address for media.

For more information on these IP addressing modes, see SIP Trunks Using Delayed Offer, page 7-14.

*Figure 7-2 Configuring the IP Addressing Mode*




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

Cisco recommends **IPv4 and IPv6** as the setting for the IP Addressing Mode for IPv6 SIP trunks. **IPv6 Only** is not recommended for production environments.

## SIP Trunk IP Addressing Mode Preference for Signaling

You can configure the IP Addressing Mode Preference for Signaling to one of the following settings (see Figure 7-3):

- IPv4

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

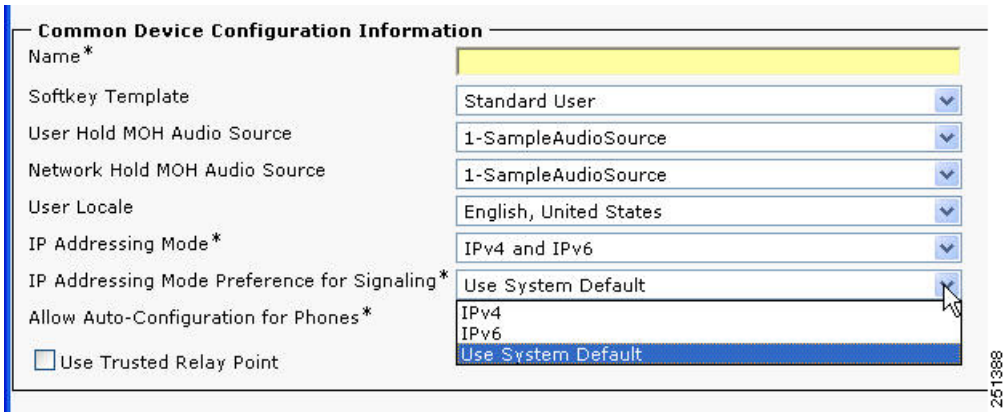
- IPv6

  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.

*Figure 7-3 Configuring the IP Addressing Mode Preference 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 will adopt 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.

#### Allow Auto-Configuration for Phones

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

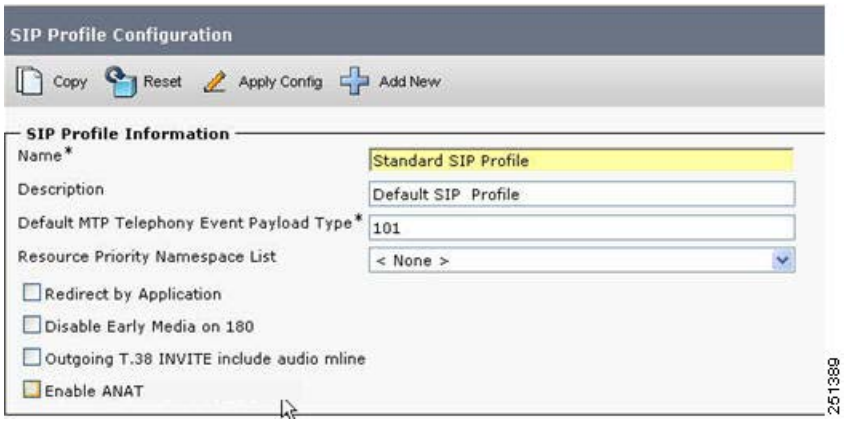
# Alternative Network Address Types (ANAT)

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.

Cisco supports 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 (see Figure 7-4). 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**.

*Figure 7-4 Enabling ANAT in the SIP Trunk Profile*




For more information on ANAT, see Alternative Network Address Types (ANAT), page 7-10.

### 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. For more information, see Media Address Selection for Calls over Dual-Stack SIP Trunks, page 7-7.

# 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. In the majority of cases, this far-end SIP trunk device will be another Unified CM cluster, IPv6 SIP gateway, or third-party IPv6 SIP call agent.

For general guidance on IPv6 SIP trunk configuration, Cisco recommends the following:

- 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, it must be supported by both trunk devices.

SIP Early Offer and SIP Delayed Offer are supported, both in symmetric and asymmetric configurations, as follows:

- Outbound and inbound SIP Early Offer
- Outbound and inbound SIP Delayed Offer
- Outbound SIP Early Offer and inbound SIP Delayed Offer
- Outbound SIP Delayed Offer and inbound SIP Early Offer

Early Offer and Delayed Offer calls are discussed briefly below and in greater detail later in this chapter.

# 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. 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 that 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 the chapter on Media Resources and Music on Hold, page 8-1.)

# 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 will dynamically insert 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 address(es) 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 Calls

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

1. The IP Addressing Mode of the SIP trunk (IPv4 Only, IPv6 Only, or IPv4 and IPv6)
2. The configured destination address(es) of the SIP trunk (IPv4 Only, IPv6 Only, or IPv4 and IPv6)
   a. 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.
   b. 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 determine by the cluster-wide IP Addressing Mode Preference for Signaling (IPv4 or IPv6).

## IP Addressing Version Used for SIP Signaling for Inbound Calls

For inbound calls, the IP addressing version used for signaling is based on the trunk destination address(es) and port number(s) 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

If IPv6 is enabled in the cluster, Unified CM servers will 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

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 upon:

- 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

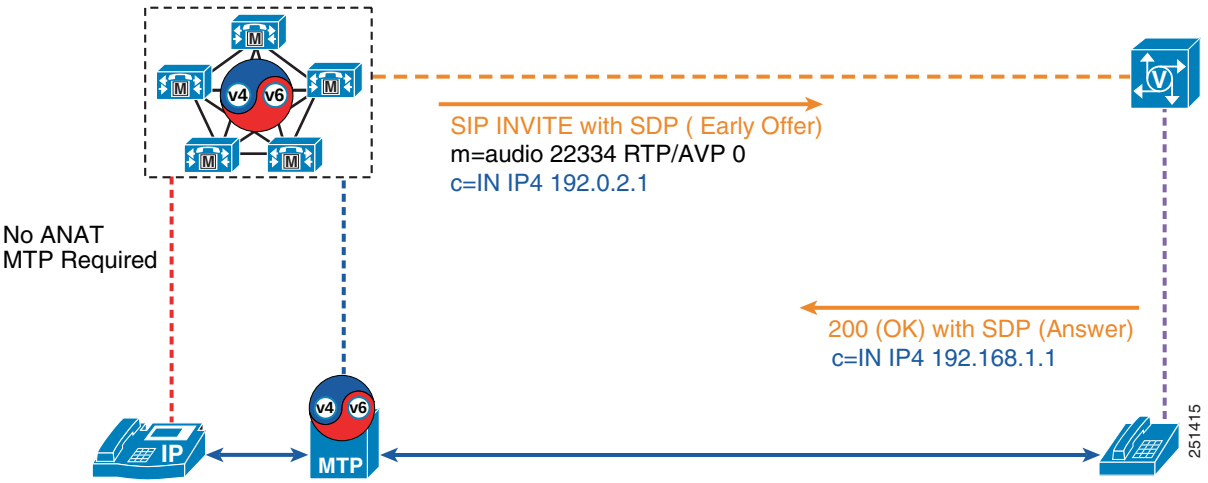
The remaining sections of this chapter review media selection for the following Unified CM call flows:

- 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 Early Offer Calls over Unified CM SIP Trunks without ANAT

As illustrated in Figure 7-5, 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 Figure 7-5, so as with a standard SIP trunk, only a single IP addressing version will be exchanged in the SIP Offer and Answer.

*Figure 7-5 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)

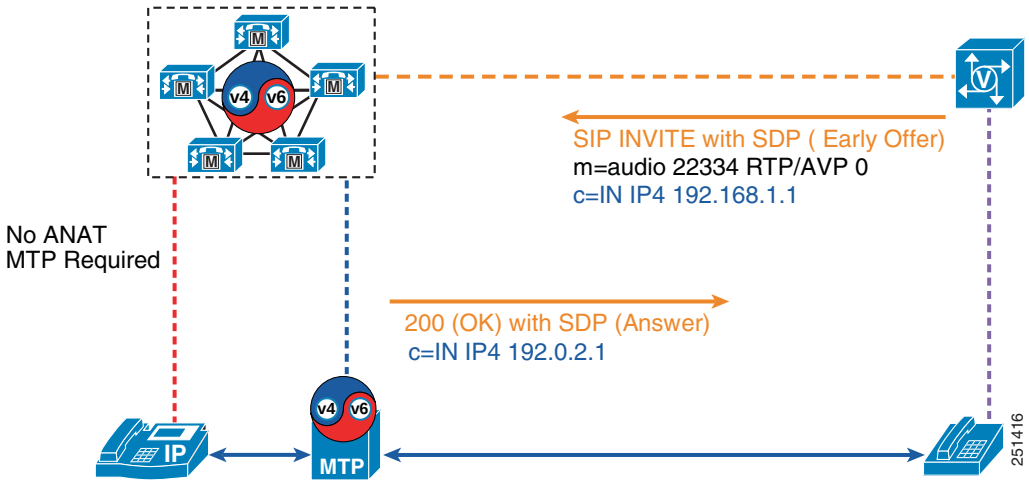
For outbound Early Offer calls where ANAT is not enabled, the IP Addressing Mode of the SIP trunk determines what is sent in the SDP body of the SIP Offer, as follows:

- 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 over Unified CM SIP Trunks without ANAT

As illustrated in Figure 7-6, 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 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 7-6 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.

- IP Addressing Mode = IPv4 and IPv6:
  - 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.

# SIP Early Offer Calls with ANAT

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.

Cisco supports 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 have an effect on how MTPs are assigned dynamically for inbound calls to Unified CM SIP trunks using Delayed Offer. (For details, see SIP Trunks Using Delayed Offer, page 7-14.)

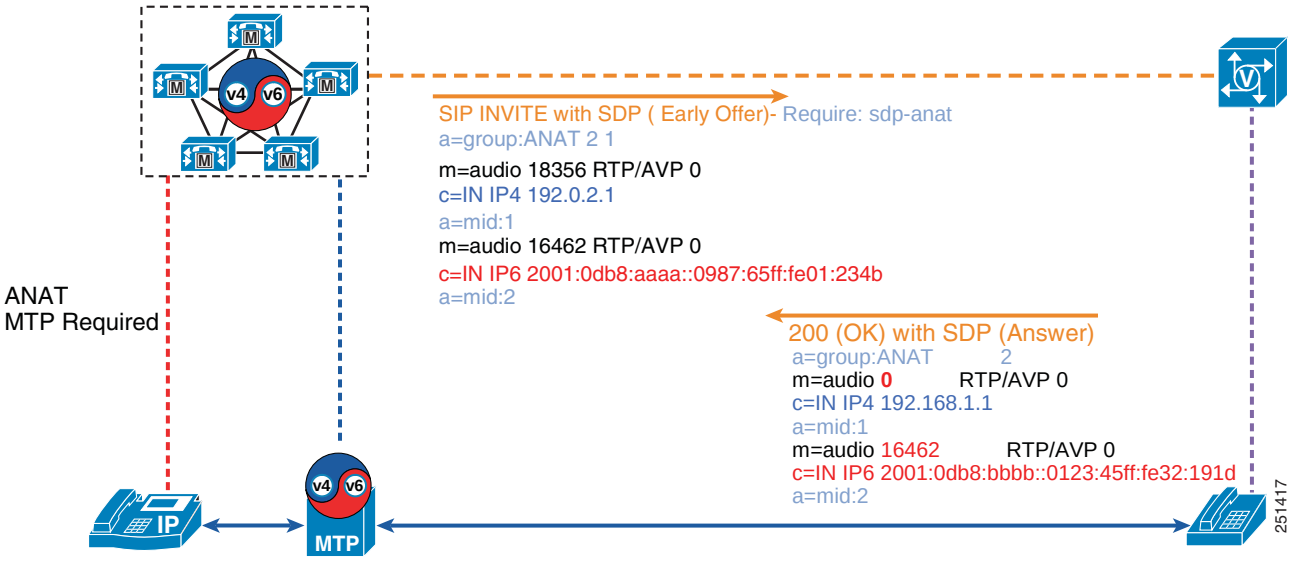
Unified CM supports ANAT over dual-stack (IPv4 and IPv6) SIP trunks. If ANAT is enabled, it should be configured on both ends of the SIP trunk. (If **Require: sdp-anat** is sent in the SIP Invite and the receiving SIP trunk does not support ANAT, all calls will be rejected.) To enable ANAT, check the **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, Cisco does not support ANAT on single-stack (IPv6 only or IPv4 only) SIP trunks.

# Media Selection for Outbound Early Offer Calls over Unified CM SIP Trunks with ANAT Enabled

Figure 7-7 shows a simplified version the SIP Early Offer and SIP Answer using ANAT on dual-stack SIP trunks.

*Figure 7-7 Media Selection on Unified CM SIP Trunks for Outbound Early Offer Calls with ANAT*




As shown in Figure 7-7, 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.

### 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. For the details of ANAT configuration on Cisco IOS gateways, see Configuring Cisco IOS Gateways, page D-1.

#### The 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.

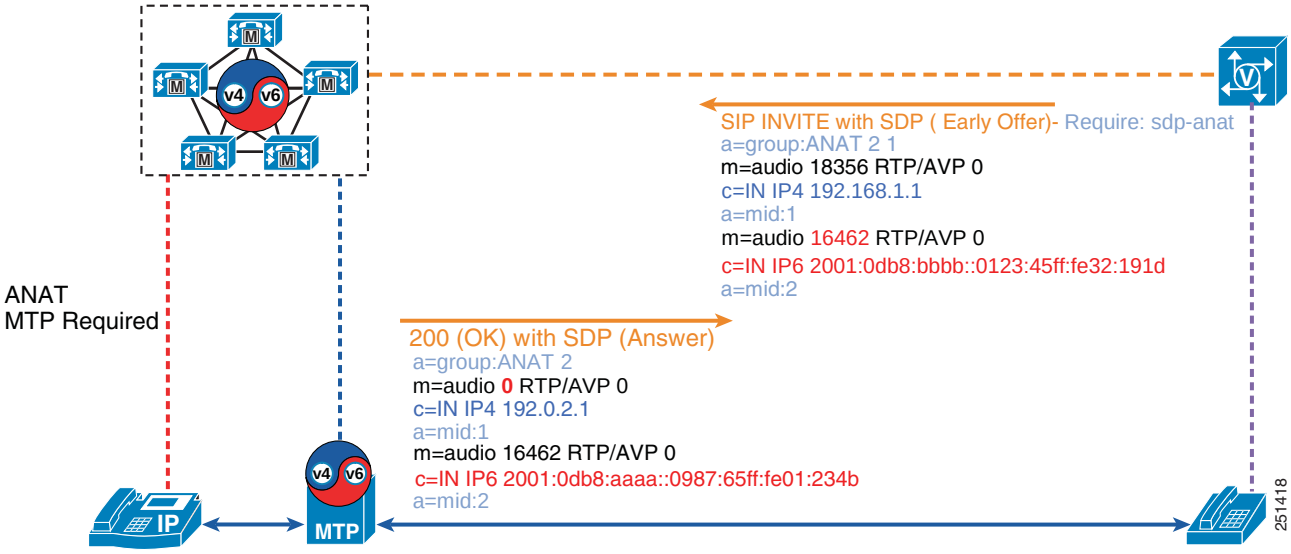
#### The Inbound SIP Answer

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 Figure 7-7, **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 over Unified CM SIP Trunks with ANAT Enabled

Figure 7-8 shows a simplified version the SIP Early Offer and SIP Answer using ANAT on dual-stack SIP trunks.

*Figure 7-8 Media Selection on Unified CM SIP Trunks for Inbound Early Offer Calls with ANAT*




As shown in Figure 7-8, 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.

### 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.

### The 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:ANAT 2 1** indicates that the second address (the IPv6 address) is preferred. For the details of ANAT configuration on Cisco IOS gateways, see Configuring Cisco IOS Gateways, page D-1.

### The 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 Figure 7-8, **a=group:ANAT 2** 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.

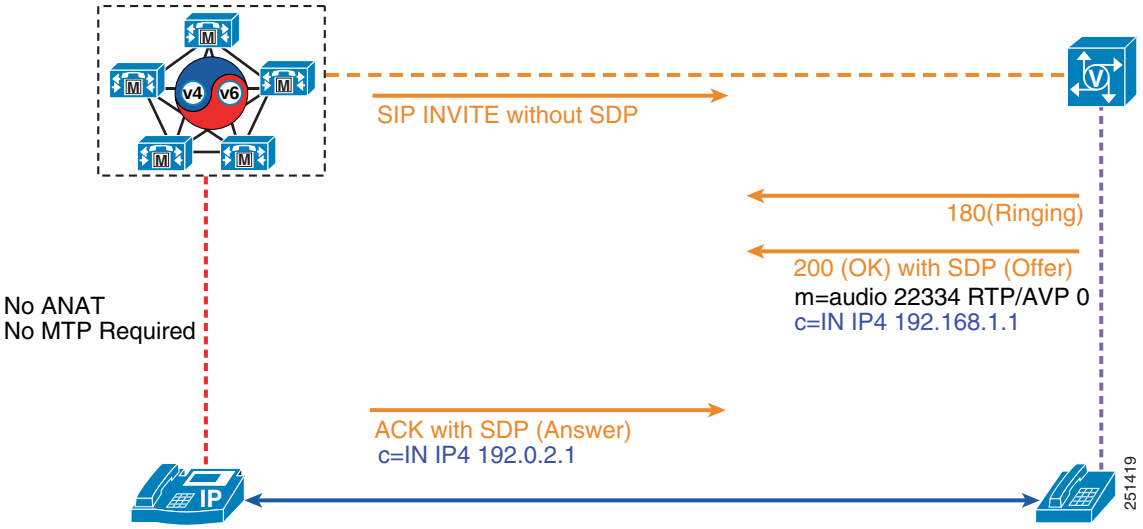
This section discusses the following call scenarios:

- Outbound Delayed Offer calls without ANAT
- Inbound Delayed Offer calls without ANAT
- Outbound Delayed Offer calls with ANAT
- Inbound Delayed Offer calls with ANAT and where **Supported: sdp-anat** is received
- Inbound Delayed Offer calls with ANAT and where **Require: sdp-anat** is received

# Media Selection for Outbound Delayed Offer Calls over Unified CM SIP Trunks without ANAT

As shown in Figure 7-9, 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 7-9 Media Selection on Unified CM SIP Trunks for Outbound Delayed Offer Calls without ANAT*




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 will be 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.

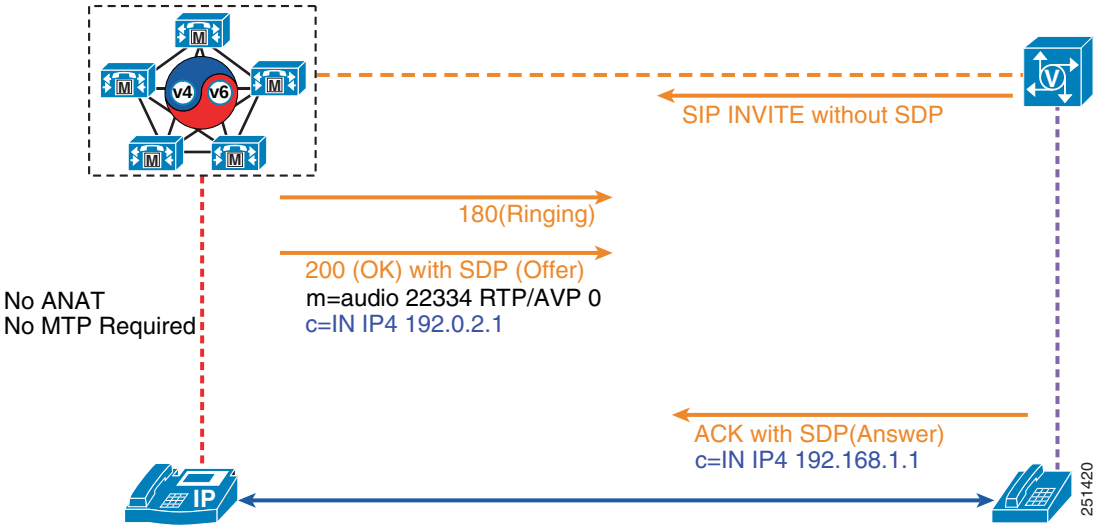
#### Deployment Considerations for Delayed Offer Calls over Trunks without ANAT

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 will dynamically insert 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 will require an MTP for conversion between IPv4 and IPv6. Therefore, Cisco recommends 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 Figure 7-10, 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 7-10 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 Table 7-1). 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 7-1 IP Addressing Mode Preference for Media*

| IP Addressing Mode of Phone | IP Addressing Mode of Trunk | Address Sent in SIP Offer by Unified CM |
|---|---|---|
| IPv4Only | IPv4Only | IPv4 address of phone |
| IPv4Only | IPv4 and IPv6 | IPv4 address of phone |
| IPv6Only | IPv6Only | IPv6 address of phone |
| IPv6Only | IPv4 and IPv6 | IPv6 address of phone |
| IPv4Only | IPv6Only | Insert an MTP and use its IPv6 address |
| IPv6Only | IPv4Only | Insert an MTP and use its IPv4 address |
| IPv4 and IPv6 | IPv4Only | IPv4 address of phone |
| IPv4 and IPv6 | IPv6Only | IPv6 address of phone |
| IPv4 and IPv6 | IPv4 and IPv6 | IPv4 or IPv6 address of phone[1] |

1. 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 Enabled

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 addressees 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 address(es) 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 will insert 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.

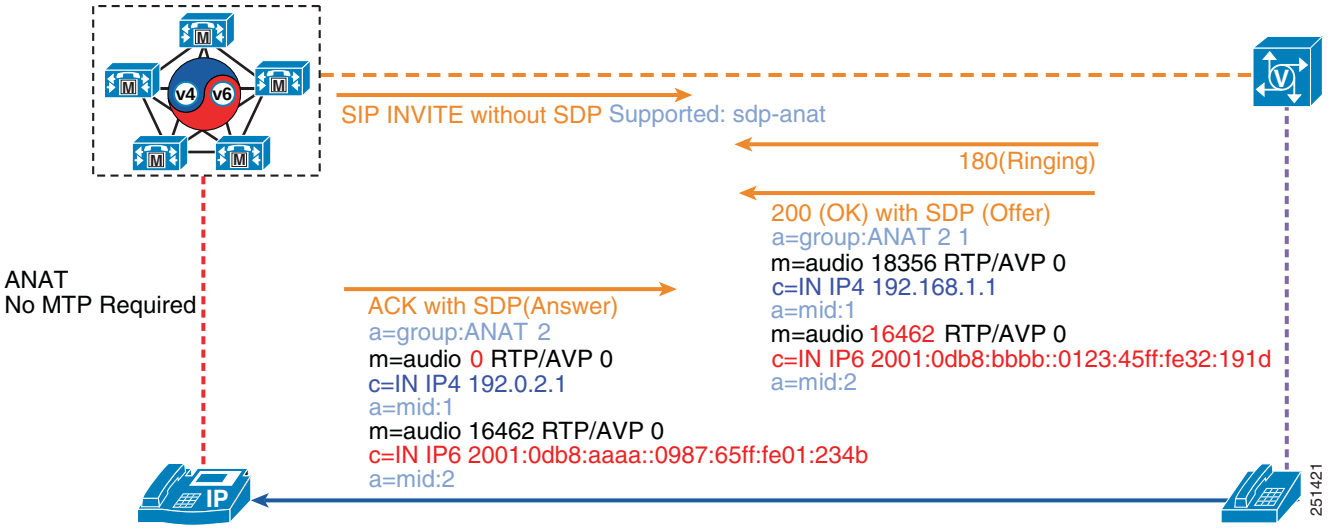
Unified CM supports ANAT over dual-stack (IPv4 and IPv6) SIP trunks. If ANAT is enabled, it should be configured on both ends of the SIP trunk. (If **Require: sdp-anat** is sent in the SIP Invite and the receiving SIP trunk does not support ANAT, all calls will be rejected.) To enable ANAT, check the **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 over Unified CM SIP Trunks with ANAT Enabled

Figure 7-11 shows a simplified version of the SIP Delayed Offer and SIP Answer using ANAT on dual-stack SIP trunks.

*Figure 7-11 Media Selection on Unified CM SIP Trunks for Outbound Delayed Offer Calls with ANAT*




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.

### The 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 the section on Media Selection for Outbound Delayed Offer Calls over Unified CM SIP Trunks without ANAT, page 7-15).

### The 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

For the details of ANAT configuration on Cisco IOS gateways, see Configuring Cisco IOS Gateways, page D-1.

### The 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 Figure 7-11, 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 (see Table 7-2).

*Table 7-2 Address(es) Sent in the SIP Answer from a Dual-Stack ANAT-Enabled Unified CM SIP Trunk*

| IP Addressing Mode of Phone | IP Addressing Mode of Trunk | Address Sent in SIP Answer by Unified CM |
|---|---|---|
| IPv4 | IPv4 and IPv6 | IPv4 address of the phone |
| IPv6 | IPv4 and IPv6 | IPv6 address of the phone |
| IPv4 and IPv6 | IPv4 and IPv6 | IPv4 and IPv6 addresses of phone[1] |

1. 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 address(es) supported by the called device.

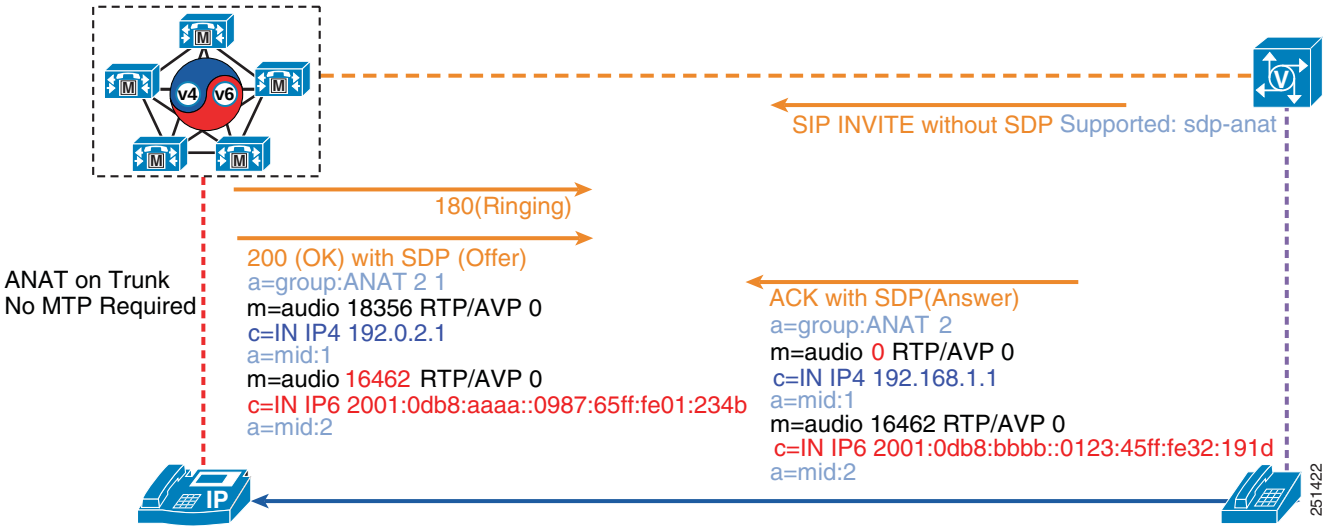
For inbound calls to ANAT-enabled dual-stack Unified CM SIP trunks where **Supported: sdp-anat** is received in the SIP Invite, Unified CM does not have to use MTPs; whereas when **Require: sdp-anat** is received by Unified CM, MTPs must be used for single-stack (IPv4-only or IPv6-only) endpoints. These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

**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.

# Media Selection for Inbound Delayed Offer Calls over Unified CM SIP Trunks with ANAT Enabled and "Supported: sdp-anat" in the Inbound SIP Invite

Figure 7-12 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 7-12 Media Selection on Unified CM SIP Trunks for Inbound Delayed Offer Calls with ANAT and Supported: sdp anat*




### The 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 **protocol mode dual-stack preference** CLI command.

For the details of ANAT configuration on Cisco IOS gateways, see Configuring Cisco IOS Gateways, page D-1.

### The 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 Figure 7-12, 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.

#### The 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 Figure 7-12, 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. (See Table 7-3.)

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

*Table 7-3 Address(es) Sent in the SIP Offer from a Dual-Stack ANAT-Enabled Unified CM SIP Trunk*

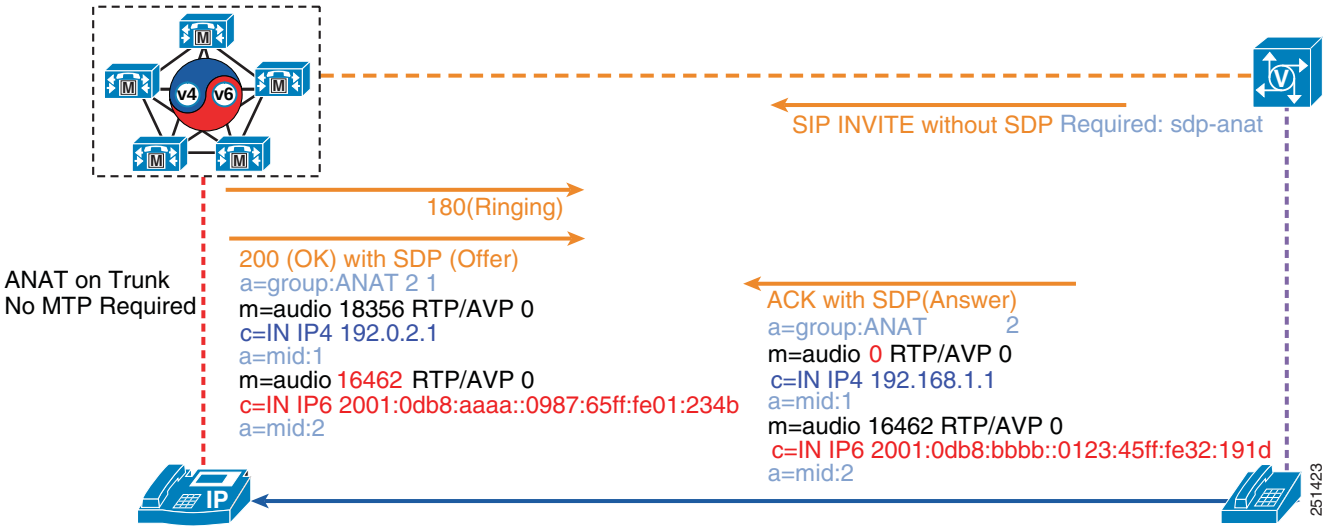
| IP Addressing Mode of Phone | IP Addressing Mode of Trunk | Address Sent in SIP Offer from Unified CM |
|---|---|---|
| IPv4 | IPv4 and IPv6 | IPv4 address of phone |
| IPv6 | IPv4 and IPv6 | IPv6 address of phone |
| IPv4 and IPv6 | IPv4 and IPv6 | IPv4 and IPv6 addresses of phone |

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.

# Media Selection for Inbound Delayed Offer Calls over Unified CM SIP Trunks with ANAT Enabled and "Require: sdp-anat" in the Inbound SIP Invite

Figure 7-13 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.

*Figure 7-13 Media Selection on Unified CM SIP Trunks for Inbound Delayed Offer Calls with ANAT and Require: sdp anat*




### The 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 **protocol mode dual-stack preference** CLI command.

For the details of ANAT configuration on Cisco IOS gateways, see Configuring Cisco IOS Gateways, page D-1.

### The 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 as well as its IPv6 address in the SDP body of the SIP Offer. For the call shown in Figure 7-13, 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:ANAT 2 1** 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.

### The Inbound SIP Answer

When ANAT is required by the calling trunk, it will send an ANAT-based response in its SIP answer. 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.

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 (see Table 7-4). 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 7-4 Address(es) Sent in the SIP Offer from a Dual-Stack ANAT-Enabled Unified CM SIP Trunk*

| IP Addressing Mode of Phone | IP Addressing Mode of Trunk | Address sent in SIP Offer from Unified CM |
|---|---|---|
| IPv4 | IPv4 and IPv6 | Insert MTP, and send IPv4 and IPv6 addresses of MTP |
| IPv6 | IPv4 and IPv6 | Insert MTP, and send IPv4 and IPv6 addresses of MTP |
| IPv4 and IPv6 | IPv4 and IPv6 | IPv4 and IPv6 addresses of phone |

CHAPTER 8

# Media Resources and Music on Hold

**Revised: June 08, 2010; OL-19142-02**

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/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 Unified Communications deployments: namely, the capability of Cisco IOS MTPs to convert a voice media stream from IPv4 to IPv6 and vice versa. 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 Unified Communications 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 12.4(22)T supports the above 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 vice versa. 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 vice versa.

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
!
```

Figure 8-1 shows when an MTP is inserted between two devices to convert from IPv4 to IPv6, and vice versa. Note, however, that 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 (see Figure 8-2). 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 (see Figure 8-3). 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 will match the longest call leg between the two devices in the cluster.

*Figure 8-1 MTP Insertion for Address Conversion Between IPv4 and IPv6*

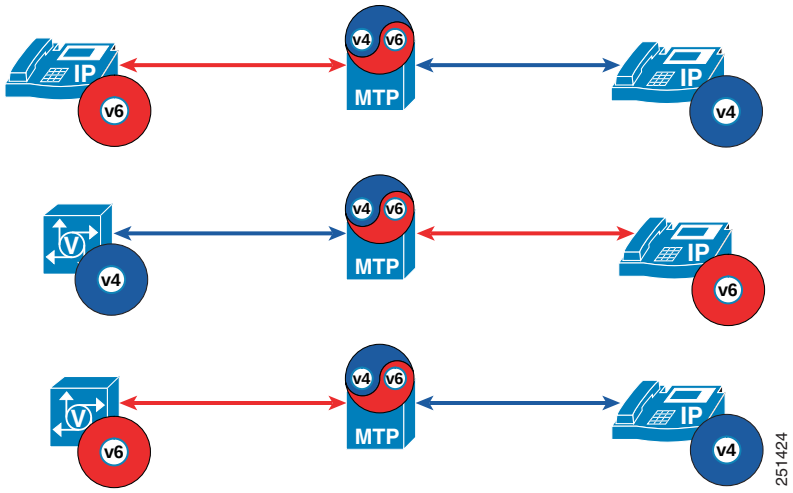



*Figure 8-2 Unified CM Chooses MTP of the IPv4 Device*

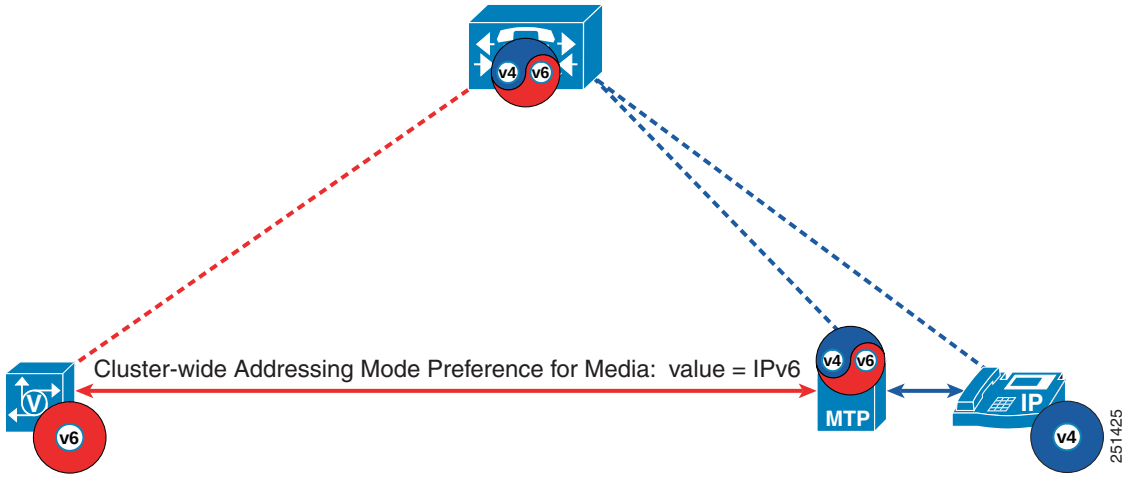
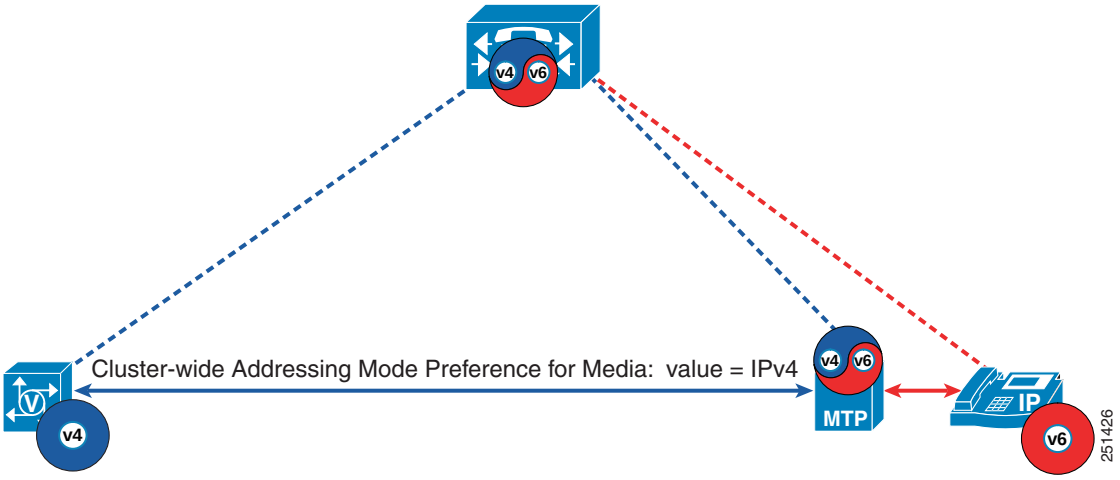


*Figure 8-3 Unified CM Chooses MTP of the IPv6 Device*




**Note** If the preferred device's MTP is not available, the other device's MTP will be used as a last resort. If no MTPs are available, the call will fail.

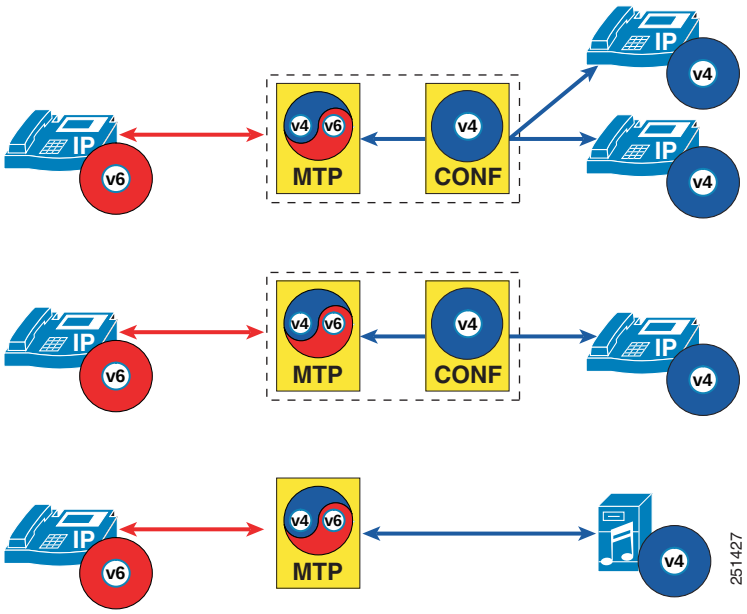
Transcoder DSP resources can also be used as hardware MTPs. If both transcoding resources and software MTPs exist in the same media resource group, Unified CM uses these media resources in a round-robin fashion for conversions between IPv4 and IPv6. To prioritize transcoding DSP resources for transcoding 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).

# 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 Figure 8-4.

- Audio conferencing
- Video conferencing
- Secure conferencing
- Transcoding
- Trusted Relay Point
- Annunciator
- Cisco IP Voice Media Streaming Application
- Music on Hold (MoH)

*Figure 8-4 MTP Inserted for Conversions Between IPv4 and IPv6*




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 an dIPv6 can occur only for the codec specified on the MTP (G.711 or G.729).

CHAPTER 9

# Call Processing and Call Admission Control

**Revised: June 08, 2010; OL-19142-02**

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 Unified Communications Solution Reference Network Design (SRND)*, available at http://www.cisco.com/go/ucsrnd.

## Enabling Call Processing for IPv6

To enable call processing for IPv6, you must first enabled 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.

### Configuring IPv6 in the CLI of Each Server in the Cluster

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:

- Enable IPv6 by using the **set network ipv6 service enable** command.
- 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.

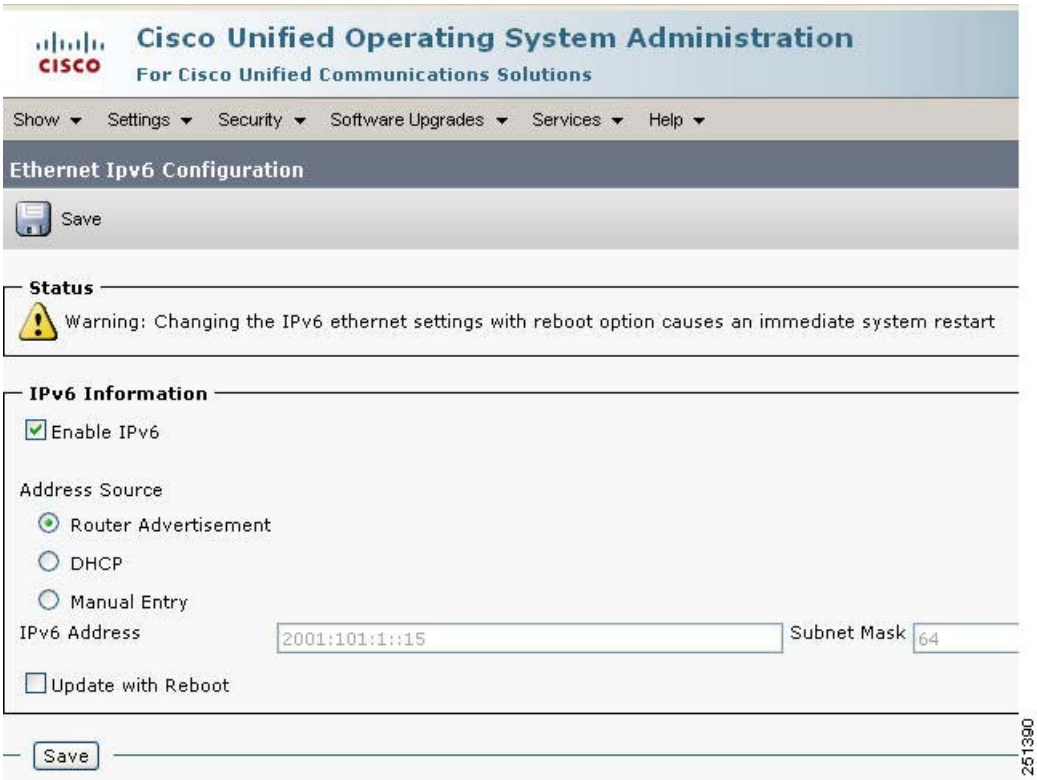
- To view the platform's IPv6 address settings, use the **show network ipv6 settings** command. Example output from this command is as follows:

```
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
```

## Configuring the Unified CM Server IPv6 Address in Cisco Unified Operating System Administration

Figure 9-1 shows how to configure the IPv6 address of the server platform by using the Cisco Unified Operating System Administration GUI. To set the address, select **Settings > IP > Ethernet IPv6**.

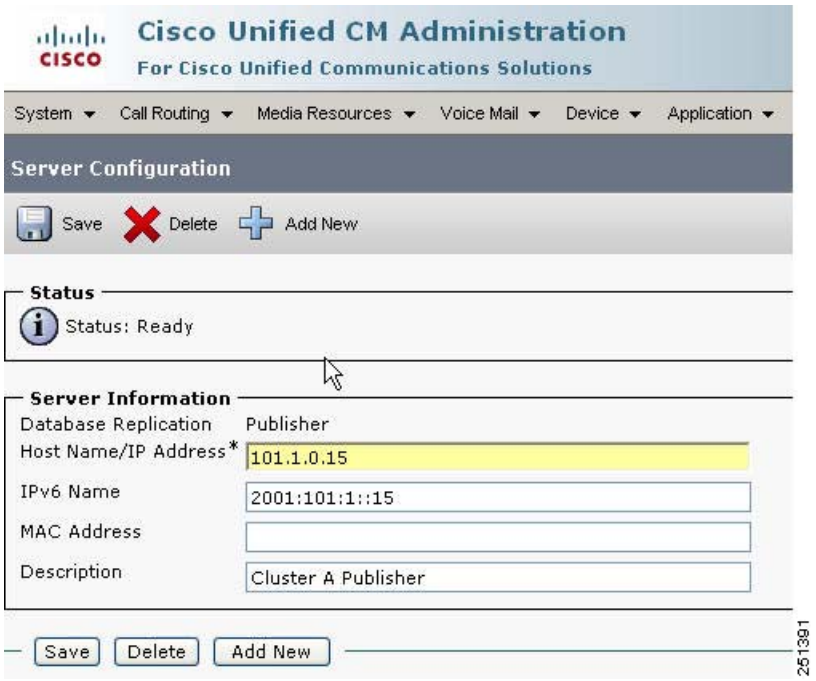
***Figure 9-1 Configuring the Server Platform IPv6 Address in Cisco Unified Operating System Administration***




## Configuring Unified CM Server IPv6 Addresses in Unified CM Administration

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 (see Figure 9-2). This IPv6 address allows SCCP phones to retrieve the IPv6 address of this Unified CM from the configuration file downloaded from the TFTP server.

*Figure 9-2 Configuring the Unified CM Server IPv6 Address in Unified CM Administration*




# 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 Configuration Modes in Unified CM Administration (see Figure 9-3):

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

*Figure 9-3 Cluster-Wide IPv6 Configuration Modes*

#### 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

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 the chapter on Media Resources and Music on Hold, page 8-1.

#### 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

#### 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 are capable of supporting IPv6. Unified CM clusters utilize 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 Unified Communications Solution Reference Network Design (SRND)*, available at http://www.cisco.com/go/ucsrnd.

## NIC Teaming for Network Fault Tolerance

NIC teaming for Network Fault Tolerance with Cisco 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 Cisco 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

Unified CM's CTI interface is IPv6-aware. This means that the CTI interface communicates with IPv4 addresses, but it can receive and understand IPv6 addresses embedded in application protocol data units (PDUs).

## Unified CM AXL/SOAP

Unified CM's Administrative XML (AXL) Simple Object Access Protocol (SOAP) interface is IPv6-aware. This means that 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 is IPv6-aware and communicates with IPv4 addresses, but it can receive and understand IPv6 addresses embedded in application protocol data units (PDUs). The SNMP Management Information Base (MIB) for Unified CM supports IPv6 addresses for IPv6-only IP phones and for dual-stack phones.

## Cisco Unified Communications Applications

The majority of Cisco Unified Communications applications support IPv4 addressing only. The exception to this is Cisco Unified Provisioning Manager, which is IPv6-aware.

## Unified CM Platform Capacity Planning

IPv6 addresses require additional Unified CM server memory when compared with IPv4 addresses. With respect to this additional overhead in a Unified CM deployment with a large number of IPv6 devices, the busy hour call completion (BHCC) capacity is approximately 3% to 5% less than the capacity of IPv4-only deployments.

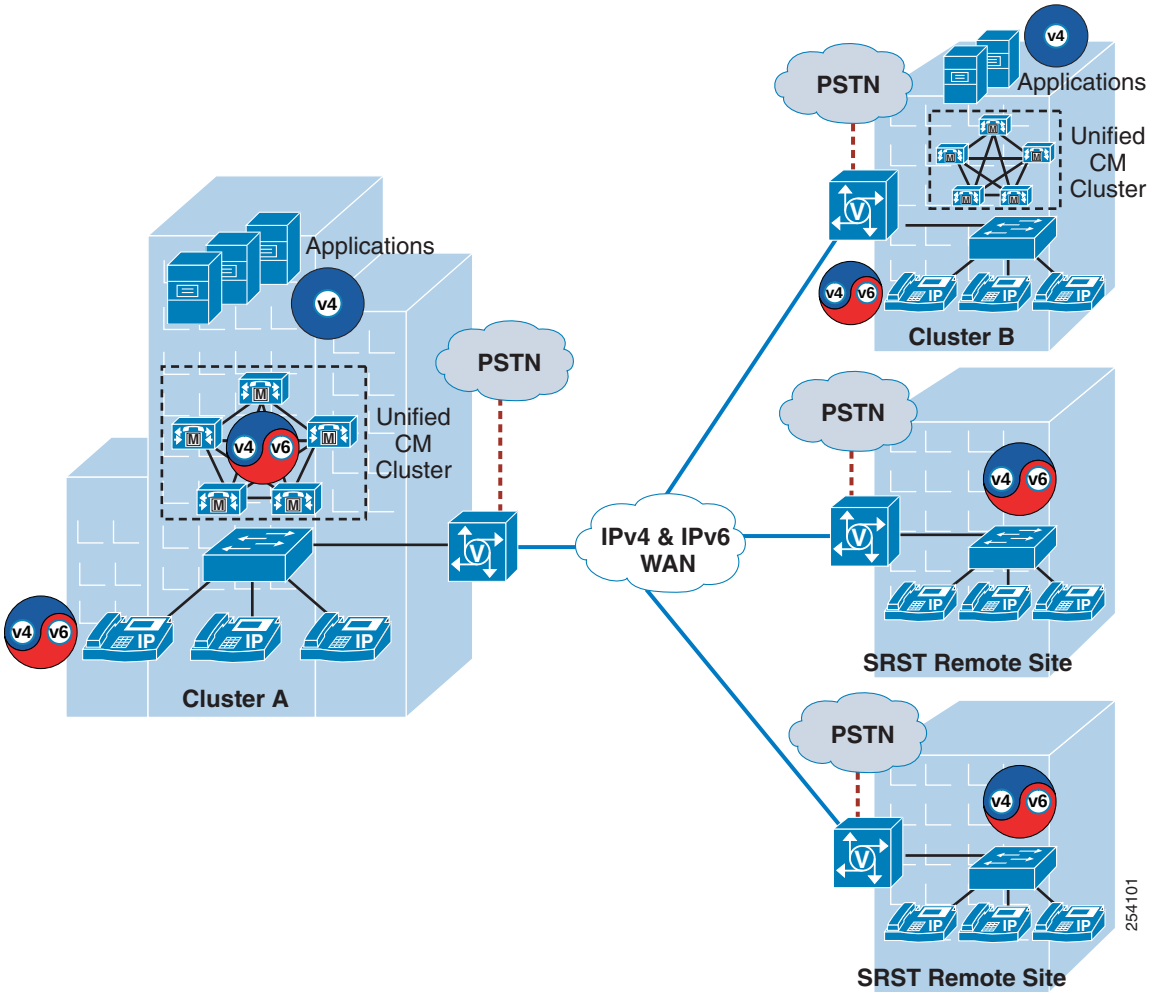
## Interoperability of Unified CM and Unified CM Express

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

# Call Admission Control

IPv6-enabled Cisco Unified CM 8.0 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 Cisco Unified CM clusters (see Figure 9-4).

*Figure 9-4 Multi-Site Unified Communications Deployment*




# Call Admission Control with Unified Communications IPv6 Deployments

Unified Communications IPv6 deployments with Cisco Unified CM 8.0 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 keeping track of the bandwidth available between any two sites in the

WAN. For general guidance on topology-unaware call admission control, refer to the *Cisco Unified Communications 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, this means the following:

- 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 5-1 in its locations-based call admission control algorithm.

# Locations-Based Call Counting Call Admission Control

Cisco Unified CM 8.0 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.

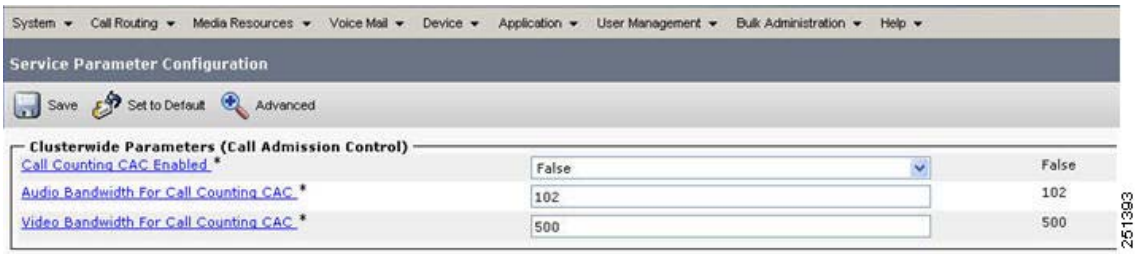
For call counting, the following default values are used for Layer 3 voice and video bandwidth when calculating the amount of available bandwidth at a location:

- 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)**. (See Figure 9-5.) The default setting for **Call Counting CAC Enabled** is False. The voice and video bandwidth values for call counting are configurable.

***Figure 9-5 Configuring Call Counting***



# Cisco Unified Communications Manager Business Edition

Cisco Unified Communications Manager Business Edition supports IPv4 only.

CHAPTER 10

# Dial Plan

**Revised: June 08, 2010; OL-19142-02**

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

  In some cases, 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).

For general dial plan guidance and design considerations, refer to the *Cisco Unified Communications Solution Reference Network Design (SRND)*, available at http://www.cisco.com/go/ucsrnd.

# 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

Cisco 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:

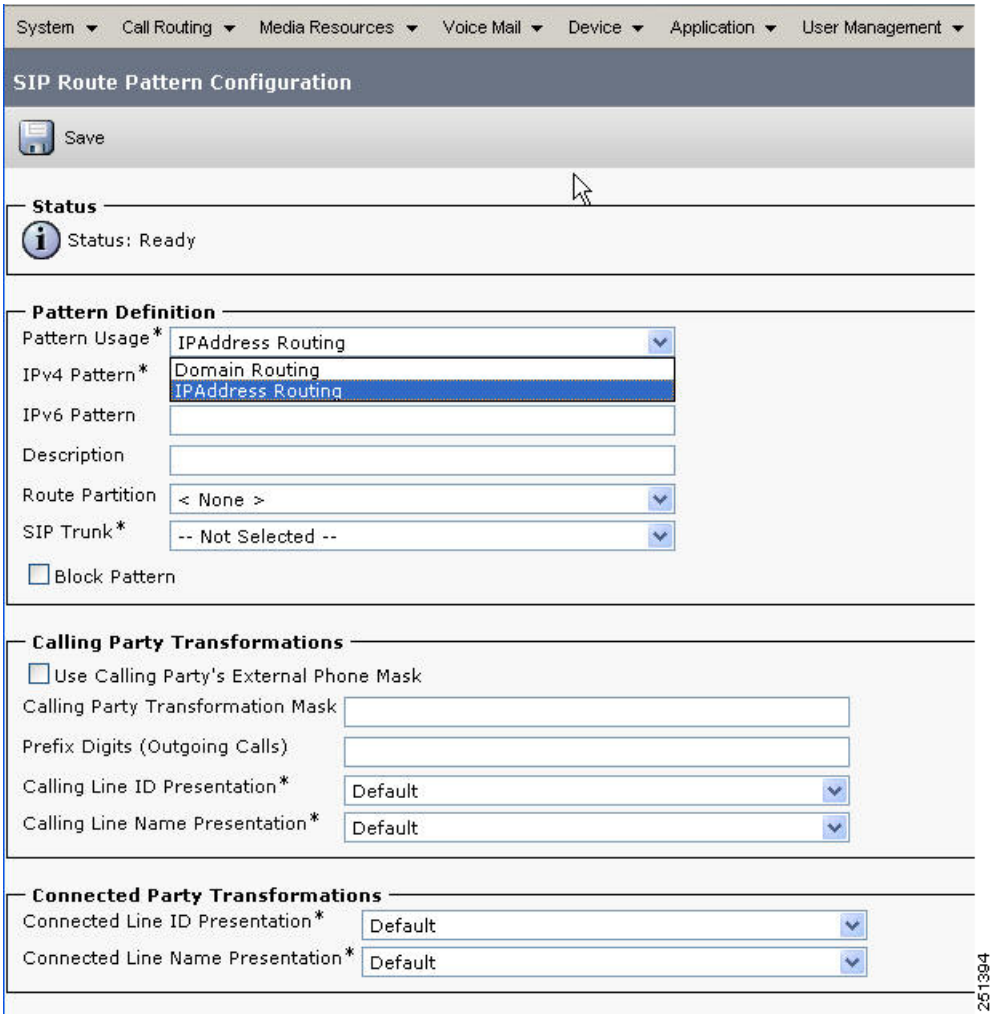
  INVITE sip:5001@2001:0db8:2::1 5060 SIP/2.0

- 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 Figure 10-1. This method allows requests that are destined for these domains to be routed through particular SIP trunk interfaces.

***Figure 10-1 SIP Route Pattern Configuration in Unified CM***



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 with SIP 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 target ipv6:[2001:db8:caf0:101:21b:78ff:fe7a:5d86]
 session transport tcp
 dtmf-relay rtp-nte
 no vad
```

For a complete example of Cisco IOS ANAT configuration and IPv6 dial peers, see Configuring Cisco IOS Gateways, page D-1

# Emergency Services

Cisco Emergency Responder is used to locate (by access switch or IPv4 subnet) IP devices that make emergency calls. Cisco Emergency Responder supports IPv4 only. Cisco Emergency Responder can support dual-stack devices by using the IPv4 address of the device. IPv6-only devices are not supported.

Cisco Emergency Responder interfaces with the following components:

- A Unified CM cluster by the following methods:
  - SNMP, to collect information about its configured phones
  - JTAPI, to allow for the call processing associated with redirection of the call to the proper PSAP gateway
- The access switches (through SNMP) where the phones associated with Unified CM are connected.

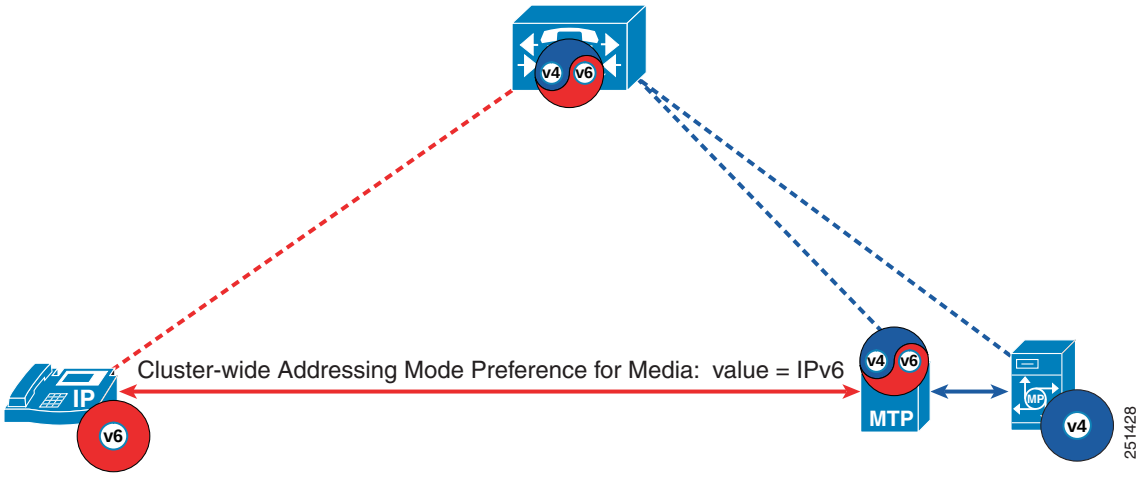
CHAPTER 11

# Applications

**Revised: June 08, 2010; OL-19142-02**

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 Figure 11-1.

***Figure 11-1 MTP Inserted for Conversion Between IPv6 and IPv4***




### Voicemail

Cisco Unity, Cisco Unity Connection, and Cisco Unity Express support IPv4 only.

### Cisco MeetingPlace

Cisco Meeting Place and Cisco Meeting Place Express support IPv4 only.

### LDAP Directory Integration

Unified CM supports only IPv4 with Lightweight Directory Access Protocol (LDAP).

### Native Unified CM Applications

Extension Mobility, IP Phones Services, Cisco Unified Communications Manager Assistant, Cisco Unified Communications Attendant Console, and WebDialer support IPv4 only.

### Device Mobility

Device Mobility is supported only for IPv4 and dual-stack devices. Currently, Unified CM Device Mobility does not support the configuration of IPv6 subnets.

### Cisco Unified Presence

Cisco Unified Presence Server, Cisco Unified Presence Client, and Cisco IP Phone Messenger support IPv4 only.

### Cisco Unified Mobility Applications

Mobility applications do not support IPv6; only IPv4 is supported.

CHAPTER 12

# IP Video Telephony

**Revised: June 08, 2010; OL-19142-02**

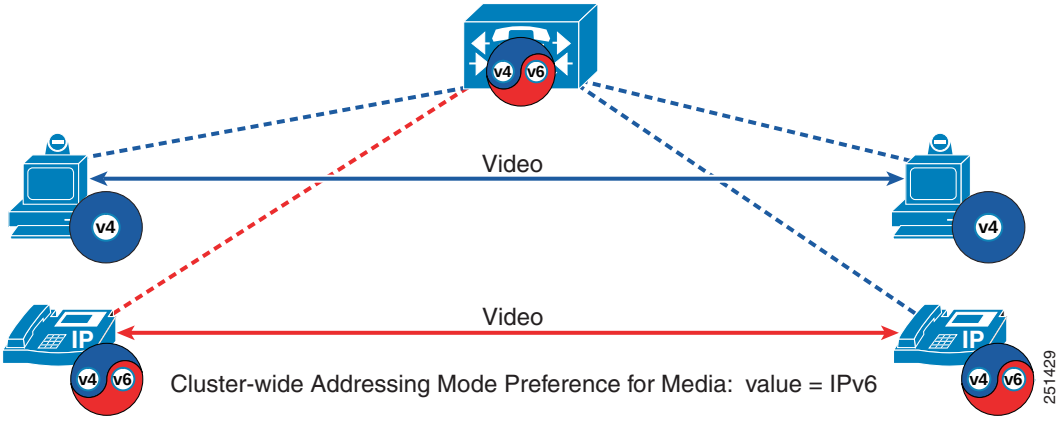
All Cisco Unified Communications video endpoints and video applications support IPv4 only for video streams. In the majority of cases, calls between video phones use IPv4 for both voice and video media streams. There is one exception, however, which involves calls using Cisco Unified Video Advantage.

Cisco Unified Video Advantage is a Windows-based application and USB camera that you can install on a personal computer running Microsoft Windows. When the PC is physically connected to the PC port of a Cisco Unified IP Phone running the Skinny Client Control Protocol (SCCP), the Cisco Unified Video Advantage application "associates" with the phone, thus enabling users to operate their phones as they always have but now with the added benefit of video. Cisco Unified Video Advantage can also be associated to Cisco IP Communicator running SCCP on the same PC, in which case both voice and video streams will use IPv4).

Unlike all other Cisco video endpoints, when Cisco Unified Video Advantage is used in conjunction with an IP phone, the voice and video media streams do not originate from the same device. In this case, the voice streams originate and terminate on the IP phones, and the video streams originate and terminate on the PCs hosting the Cisco Unified Video Advantage camera.

Video streams from all Cisco video devices support IPv4 only. In the case of Cisco Unified Video Advantage, IPv4 is used for its video stream, but the IP addressing version used to transport the voice media between the IP phones may be IPv4 or IPv6. The IP addressing version used for the voice streams depends upon the capabilities of the phones, the addressing mode settings of the phones, and the cluster-wide IP Addressing Mode Preference for Media (in the case of a call between two dual-stack phones). Figure 12-1 shows an example of addressing mode selection with Cisco Unified Video Advantage.

*Figure 12-1 Addressing Modes for Voice and Video Media Streams with Cisco Unified Video Advantage*




Video calls can be made across ANAT-enabled dual-stack SIP trunks that are configured to use Delayed Offer. In the majority of cases, both the voice and video streams for these calls will use IPv4. The exception mentioned previously for Cisco Unified Video Advantage also applies to calls over SIP trunks, in which case SIP will negotiate IPv4 for video and can negotiate either IPv4 or IPv6 for voice.

CHAPTER 13

# IP Telephony Migration Options

**Revised: June 08, 2010; OL-19142-02**

For first-time installations of IPv6 with Cisco Unified Communications Manager (Unified CM), Cisco recommends the following guidelines:

### Deployment Models

For Cisco Unified CM 8.0, IPv6 is supported for single-site deployments, multi-site deployments with distributed call processing, and multi-site deployments with centralized call processing.

### 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 Auto-Configuration for Phones

### DHCP

Stateful DHCPv6 is recommended, although stateless DHCP can also be used in conjunction 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 dual-stack (IPv4 and IPv6) with Alternative Network Address Types (ANAT) enabled. Either Delayed Offer or Early Offer may be used. Bear in mind, however, that SIP trunks configured for Early Offer (MTP Required) use an MTP resource for every call and do not support video calls or encrypted calls.

### IP Phones

IPv6-only phones have a number of functional limitations (see Unified Communications Endpoints, page 15-1), and they should be used only for non-production purposes. IPv6-capable phones should be configured as **IPv4 only** or **IPv4 and IPv6**.

CHAPTER 14

# Security

**Revised: June 08, 2010; OL-19142-02**

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 simply replaced with neighbor discovery (ND) security issues in IPv6.

For more information on IPv6 security in campus and branch networks, refer to the security sections of the following campus and branch network IPv6 design guides:

- *Deploying IPv6 in Campus Networks*

  http://www.cisco.com/en/US/docs/solutions/Enterprise/Campus/CampIPv6.html
- *Deploying IPv6 in Branch Networks*

  http://www.cisco.com/en/US/docs/solutions/Enterprise/Branch/BrchIPv6.html

## Privacy and Encryption for IPv6 Voice Signaling and Media

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)

  TSL 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.

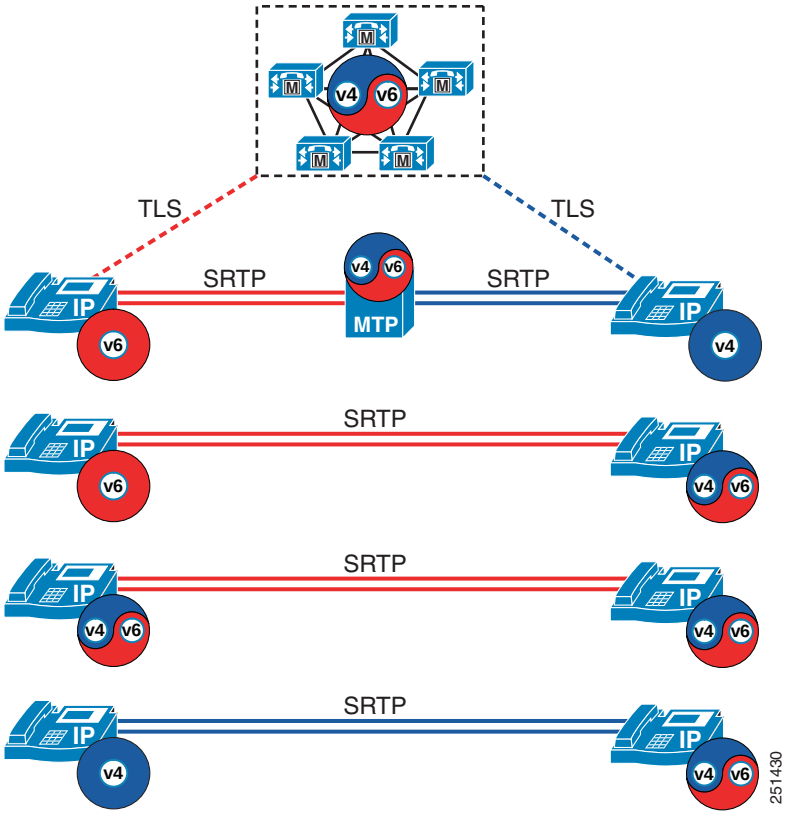
For more information on Unified CM security, refer to the *Cisco Unified Communications Manager Security Guide*, available at

http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

# 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 (see Figure 14-1). 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 vice versa.

*Figure 14-1 Addressing Mode Resolution by Unified CM*




# 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 Unified Communications Traffic and Firewalls

The Cisco IOS Firewall, Adaptive Security Appliance (ASA), and Firewall Services Module (FWSM) do not support SCCP fix-up or SIP fix-up for IPv6, therefore they cannot be used to open pinholes dynamically for IPv6 voice traffic. However, these products do support 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 IOS IPv6 Configuration Guide*

  http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-sec_trfltr_fw.html
- *Cisco ASA 5580 Adaptive Security Appliance Command Line Configuration Guide*

  http://www.cisco.com/en/US/docs/security/asa/asa81/config/guide/ipv6.html
- *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Configuration Guide*

  http://www.cisco.com/en/US/docs/security/fwsm/fwsm40/configuration/guide/ipv6_f.html

# Cisco Unified Border Element

The Cisco IOS-based Cisco Unified Border Element has the ability to:

- Terminate a SIP IPv6 call on one leg of a session, and generate a SIP or H.323 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 IPv6 networks and IPv4 networks.

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

# Cisco Security Agent

Cisco Security Agent does not support IPv6.

# Summary

Future releases of the Cisco security platforms and products mentioned in this chapter will provide support for IPv6 Unified Communications traffic. However, until these products do support IPv6 for Unified Communications traffic, Cisco recommends 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.

CHAPTER 15

# Unified Communications Endpoints

**Revised: June 08, 2010; OL-19142-02**

This chapter describes the Cisco Unified Communications endpoints and their IPv6 capabilities. Table 15-1 lists the endpoint types and summarizes their IPv6 capabilities.

*Table 15-1 IPv6 Capabilities of Unified Communications Endpoints*

| Endpoint Type | IPv6 Capability |
|---|---|
| Analog gateways | Some gateways support IPv6 |
| Cisco Unified IP Phones | Some Cisco Unified IP Phones support IPv6 |
| Software-based endpoints | No software-based endpoints support IPv6 |
| Wireless endpoints | No wireless endpoints support IPv6 |
| Cisco Unified IP Conference Station | No conference stations support IPv6 |
| Video endpoints | No video endpoints support IPv6 |
| Third-party SIP IP phones | Third-party IPv6-capable phones are not supported |

As indicated in Table 15-1, IPv6 support extends to only a subset of the Cisco analogue gateways and IP phones. The following sections discuss these devices in more detail.

# IPv6 Support on Analog Gateways

The following analog gateways support IPv6:

- Cisco VG224 Analog Voice Gateway
- Analogue FXS ports on Cisco 2800 Series and 3800 Series Integrated Services Routers

## Cisco VG224 Analog Voice Gateway

The Cisco VG224 Analog Voice Gateway is a Cisco IOS high-density 24-port gateway for connecting analog devices to the Cisco Unified Communications network. In Cisco IOS Release 12.4(22)T and later releases, the Cisco VG224 can act as an IPv6-capable Skinny Client Control Protocol (SCCP) endpoint with Cisco Unified Communications Manager (Unified CM). Once added as a gateway in Unified CM, the FXS ports on the VG224 gateway register as individual devices with Unified CM.

For configuration details about the Cisco VG224, see Configuring Cisco VG224 Analog Voice Gateway, page C-1.

## Cisco Integrated Services Router (ISR) Analog FXS Ports

Analogue FXS ports on Cisco 2800 Series and 3800 Series Integrated Services Routers can act as IPv6-capable Skinny Client Control Protocol (SCCP) endpoints with Cisco Unified Communications Manager (Unified CM). Once added as a gateway in Unified CM, the FXS ports on the router register as individual devices with Unified CM.

For configuration details about the Cisco 2800 and 3800 Series Integrated Services Router FXS ports, see Configuring Cisco Integrated Services Routers, page B-1. Use the Cisco IOS command line interface (CLI) and the Unified CM Administration graphical user interface to configure the analogue FXS ports.

# IPv6 Support on Cisco Unified IP Phones

The following SCCP-based Cisco Unified IP Phone models support IPv6:

- Cisco Unified IP Phone 7906G
- Cisco Unified IP Phone 7911G
- Cisco Unified IP Phone 7931G
- Cisco Unified IP Phone 7941G and Cisco Unified IP Phone 7941GE
- Cisco Unified IP Phone 7942G
- Cisco Unified IP Phone 7945G
- Cisco Unified IP Phone 7961G and Cisco Unified IP Phone 7961GE
- Cisco Unified IP Phone 7962G
- Cisco Unified IP Phone 7965G
- Cisco Unified IP Phone 7970G
- Cisco Unified IP Phone 7971G-GE
- Cisco Unified IP Phone 7975G

These phones models can be configured to support the following addressing modes:

- A single IPv4 address
- A single IPv6 address
- Both an IPv4 address and an IPv6 address (also known as dual-stack configuration)

For phones that support both an IPv4 address and an IPv6 address, the following conditions apply:

- For call control signaling to Unified CM, the phone can be configured to use either its IPv4 address or its IPv6 address.
- For voice media between two dual-stack devices, the devices may choose to use either their IPv4 addresses or their IPv6 addresses to transport RTP voice streams.

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 vice versa).

### 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, this can cause an IPv6 address from the voice VLAN to be assigned to the PC.

If you encounter the above 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 significantly 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) will pick the Network Prefix included in RAs with the longest lifetime, and will 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 Configuratio**n 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.

Cisco recommends 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 bits 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.

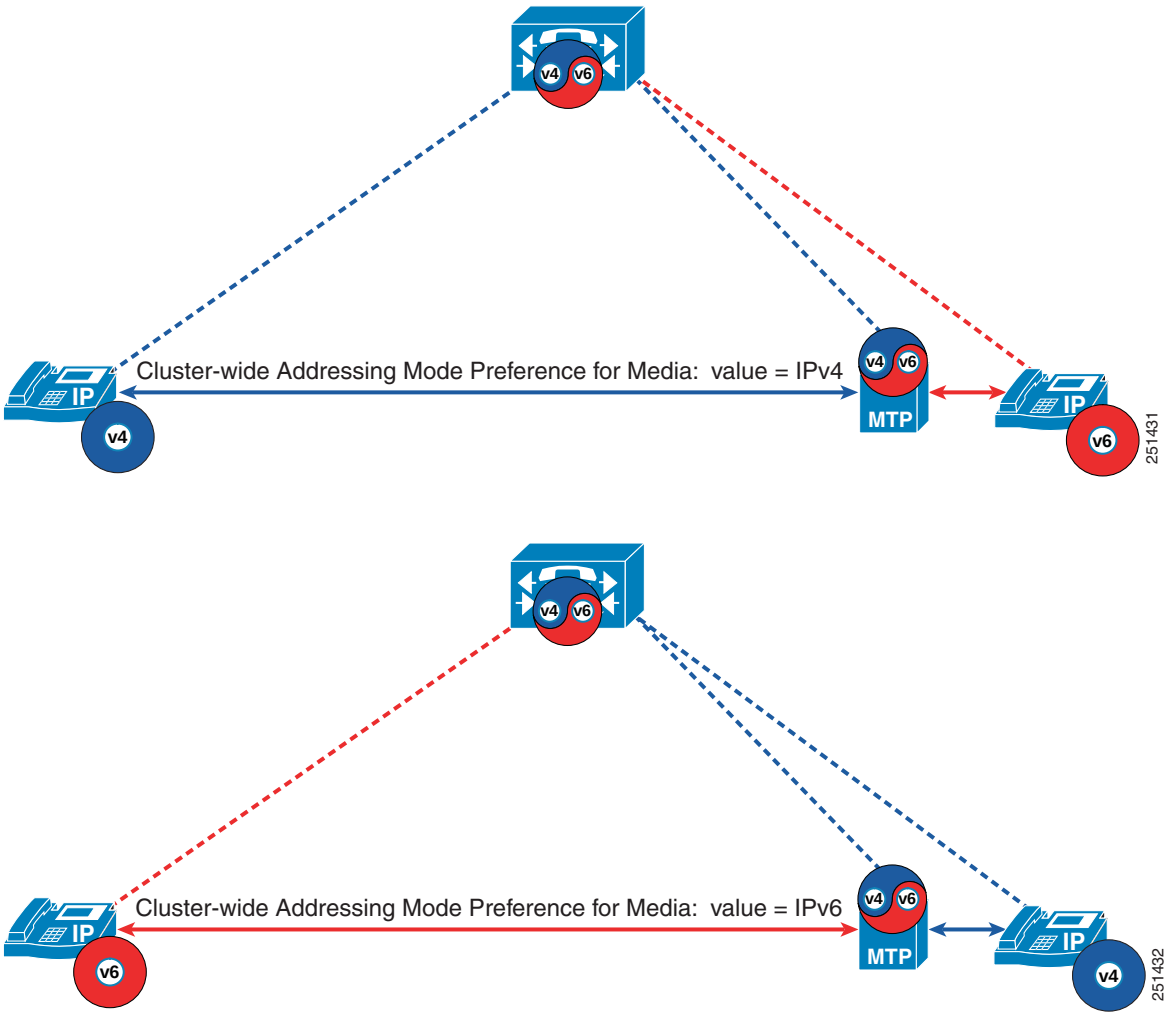
If IPv6 is enabled in the Unified CM cluster, the phone's default setting of Allow Auto-Configuration for Phones is **Default**. If the IP phone supports either IPv6 only or both IPv4 and IPv6, it will adopt the cluster-wide setting for Allow Auto-Configuration for Phones, but all IPv4-only phones will ignore this setting.

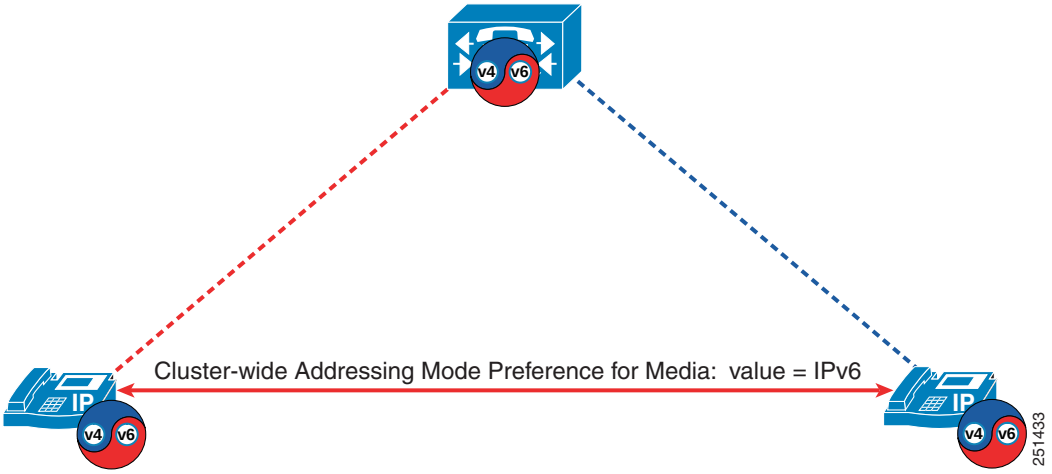
# Default Common Device Configuration Profile

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

***Figure 15-1 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 Unified 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 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 will then attempt 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. The HTTP server provides several functions, including:

- Telephone User Interface access to:
  - Directory search functions
  - Call history
  - All IP Phone Services
  - Extension Mobility

  - 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 CDP or LLDP messages.

## IPv6-Only Phones

IP phones configured with an IP addressing mode of **IPv6 Only** are subject to a number of functional limitations and are therefore not recommended for production deployments. Those limitations are described here:

- Because the phone's HTTP server uses IPv4 only, the following functions are not available to IPv6-only phones:
  - Directory search functions
  - Call history
  - All IP Phones Services
  - Extension Mobility
  - Quality Report Tool (QRT)
  - Web access to the phone through the Unified CM phone administration graphical user interface
- Device mobility uses IP subnet information to locate mobile devices. Only IPv4 subnets are supported for device mobility, and this function is not supported for IPv6-only phones.
- Peer Firmware Sharing 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.

APPENDIX A

# Configuring IPv6 in Cisco Unified CM

**Revised: June 08, 2010, OL-19142-02**

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

- Enable IPv6 by using the **set network ipv6 service enable** command.
- 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 it is not recommended.
- To view the platform's IPv6 address settings, use the **show network ipv6 settings** command. Example output from this command is as follows:

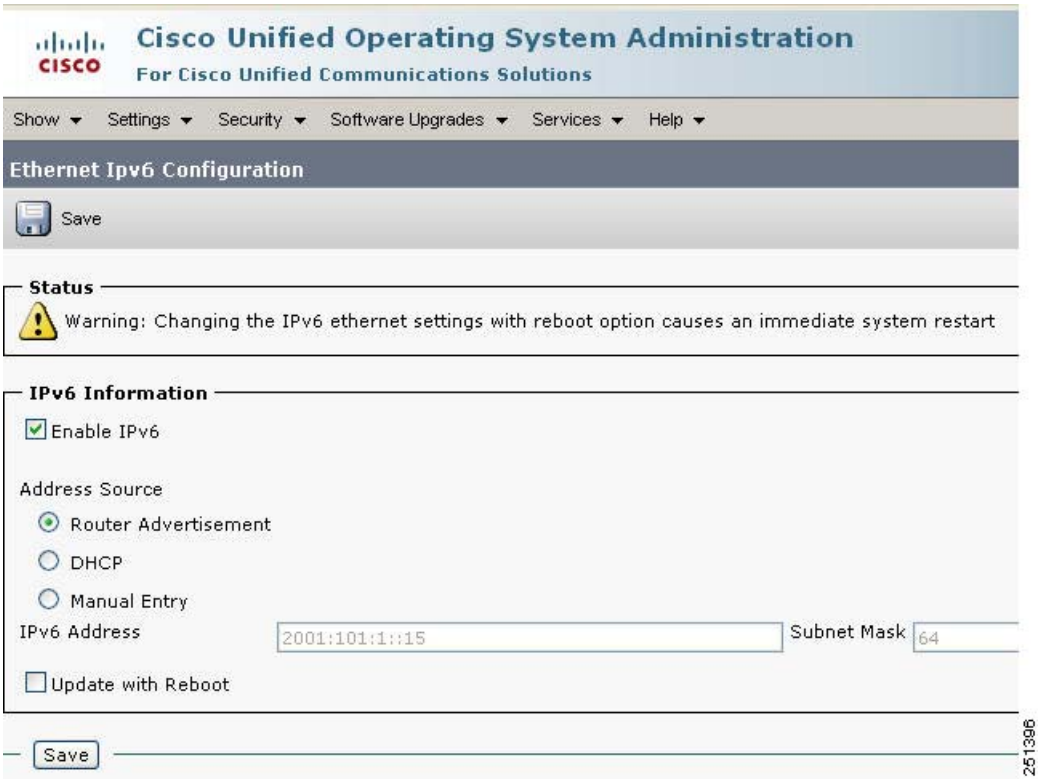
```
IPv6   : enabled
DHCPv6 : disabled
       IPv6 addresses:
    Address:2001:db8:c18:1:21c:c4ff:feef:ca0        Mask:64
    Scope:Global    Duplicate:no

    Address:fe80::21c:c4ff:feef:ca0 Mask:64
    Scope:Link
```

Next, define the IPv6 address for each Unified CM server by using Cisco Unified CM Administration to select **System > Server**, and enter the IPv6 address in the field labeled **IPv6 Name**. (See Configuring Unified CM Server IPv6 Addresses, page A-3.) The IPv6 address in this field enables Skinny Client Control Protocol (SCCP) phones to retrieve the IPv6 address of Unified CM from the configuration file downloaded from the TFTP server.

### Configuring the Unified CM Server Hardware IPv6 Address Through Cisco Unified Operating System Administration

Instead of using the server command line interface as described above, you can use Cisco Unified Operating System Administration to set the Unified CM server IPv6 address. In Cisco Unified OS Administration, select **Settings > IP > Ethernet IPv6**, as illustrated in Figure A-1.

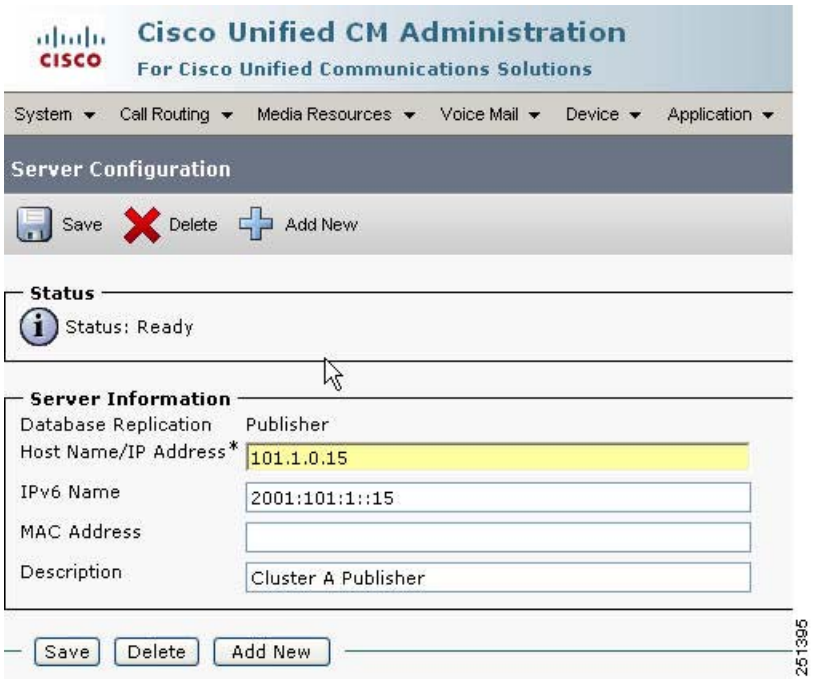
*Figure A-1 Configuring the Unified CM Server IPv6 Address Through Cisco Unified Operating System Administration*



### Configuring Unified CM Server IPv6 Addresses

After you have configured 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 (see Figure A-2). The IPv6 address in this field enables Skinny Client Control Protocol (SCCP) phones to retrieve the IPv6 address of this Unified CM from the configuration file downloaded from the TFTP server.

***Figure A-2 Configuring the Unified CM Server IPv6 Address in Unified CM Administration***



APPENDIX B

# Configuring Cisco Integrated Services Routers

**Revised: June 08, 2010, OL-19142-02**

This appendix contains IPv6 configuration examples for the following components on Cisco Integrated Services Routers (ISRs):

- IPv6 SIP trunks
- FXS ports
- Media termination point (MTP) resources

For additional information on IPv6 configuration, refer to the following documentation:

- *Cisco IOS Voice Command Reference*
  http://www.cisco.com/en/US/docs/ios/voice/command/reference/vr_book.html
- *Cisco IOS IPv6 Command Reference*
  http://www.cisco.com/en/US/docs/ios/ipv6/command/reference/ipv6_book.html

# Cisco ISR Configuration for an IPv6 SIP Trunk

```
!
boot-start-marker
boot system flash:c3845-adventerprisek9_ivs-mz.124-22.T
boot-end-marker
!
card type t1 0 0
card type t1 0 1
!
clock timezone EST -5
clock summer-time EDT recurring
network-clock-participate wic 0
network-clock-participate wic 1
!
ip source-route
ip cef
!
ipv6 unicast-routing
ipv6 cef
!
isdn switch-type primary-4ess
!
voice service voip
 sip
```

```
  bind control source-interface GigabitEthernet0/0
  bind media source-interface GigabitEthernet0/0
!
controller T1 0/1/1
 clock source internal
 cablelength long 0db
 pri-group timeslots 1-24
 description T1 PRI - SIP Trunk to CUCM
!
interface GigabitEthernet0/0
 ip address 101.1.0.2 255.255.255.0
 duplex full
 speed auto
 media-type rj45
 ipv6 address 2001:101:1:1::4/64
 ipv6 nd ra mtu suppress
 ipv6 ospf 1 area 0
 no keepalive
!
interface Serial0/1/1:23
 description PRI - SIP Trunk to CUCM - SIPv6 controlled
 no ip address
 encapsulation hdlc
 isdn switch-type primary-ni
 isdn protocol-emulate network
 isdn incoming-voice voice
 no cdp enable
!
router eigrp 101
 network 101.0.0.0
 no auto-summary
!
router ospf 1
 log-adjacency-changes
 network 101.0.0.0 0.255.255.255 area 0
!
ip forward-protocol nd
!
ipv6 router ospf 1
 log-adjacency-changes
!
voice-port 0/1/1:23
 description PRI Trunk
!
dial-peer voice 10 pots
 description SIP controlled PRI to CUCM
 destination-pattern 502T
 incoming called-number .
 direct-inward-dial
 port 0/1/1:23
!
dial-peer voice 100 voip
 destination-pattern .T
 session protocol sipv2
 session target ipv6: 2001:101:1::16
 dtmf-relay rtp-nte
 no vad
!
dial-peer voice 101 voip
 destination-pattern .T
 session protocol sipv2
 session target ipv6: 2001:101:1::15
 dtmf-relay rtp-nte
 no vad
```

```
!
sip-ua
!
end
```

# Cisco ISR Configuration for an FXS Port

```
ip source-route
!
ip cef
!
ipv6 unicast-routing
ipv6 cef
!
stcapp ccm-group 1
stcapp
!
voice service voip
!
voice-card 0
 dspfarm
 dsp services dspfarm
!
interface GigabitEthernet0/0
 no ip address
 duplex full
 speed auto
 ipv6 address 2001:101:1:1::7/64
 ipv6 nd ra mtu suppress
 ipv6 ospf 1 area 0
 no keepalive
!
router ospf 1
 log-adjacency-changes
 network 101.0.0.0 0.255.255.255 area 0
!
ip forward-protocol nd
!
ipv6 router ospf 1
 router-id 101.1.1.7
 log-adjacency-changes
!
control-plane
!
voice-port 0/0/0
 timeouts ringing infinity
!
voice-port 0/0/1
 timeouts ringing infinity
!
voice-port 0/0/2
 timeouts ringing infinity
!
voice-port 0/0/3
 timeouts ringing infinity
!
sccp local GigabitEthernet0/0
sccp ccm 2001:101:1::16 identifier 3 version 7.0
sccp ccm 2001:101:1::15 identifier 1 version 7.0
sccp
```

```
!
sccp ccm group 1
 associate ccm 1 priority 1
 associate ccm 3 priority 3
!
dial-peer voice 1 pots
 service stcapp
 port 0/0/0
!
dial-peer voice 2 pots
 service stcapp
 port 0/0/1
!
dial-peer voice 3 pots
 service stcapp
 port 0/0/2
!
dial-peer voice 4 pots
 service stcapp
 port 0/0/3
!
```

# Cisco ISR Configuration for an MTP Resource

```
boot system flash:c2800nm-adventerprisek9_ivs-mz.124-22.T
!
network-clock-participate wic 0
!
ip source-route
ip cef
!
ipv6 unicast-routing
ipv6 cef
!
voice service voip
!
voice-card 0
 dspfarm
 dsp services dspfarm
!
interface GigabitEthernet0/0
 ip address 101.1.200.2 255.255.255.252
 duplex auto
 speed auto
 ipv6 address 2001:101:1:200::2/64
 ipv6 nd ra mtu suppress
 ipv6 ospf 1 area 0
!
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0/1.112
 description VOICE VLAN
 encapsulation dot1Q 112
 ip address 101.1.1.5 255.255.255.0
 ipv6 address 2001:101:1:1::5/64
 ipv6 nd ra mtu suppress
 ipv6 ospf 1 area 0
```

```
!
interface GigabitEthernet0/1.120
 description DATA VLAN
 encapsulation dot1Q 120
 ip address 101.1.20.5 255.255.255.0
 ipv6 address 2001:101:1:20::5/64
 ipv6 nd ra mtu suppress
 ipv6 ospf 1 area 0
!
router eigrp 101
 network 101.0.0.0
 no auto-summary
!
router ospf 1
 log-adjacency-changes
 network 101.0.0.0 0.255.255.255 area 0
!
ip forward-protocol nd
!
ipv6 router ospf 1
 log-adjacency-changes
!
sccp local GigabitEthernet0/1.112
sccp ccm 101.1.0.16 identifier 2 version 7.0
sccp ccm 101.1.0.15 identifier 1 version 7.0
sccp ccm 2001:101:1::15 identifier 3 version 7.0
sccp ccm 2001:101:1::16 identifier 4 version 7.0
sccp
!
sccp ccm group 1
 associate ccm 1 priority 1
 associate ccm 2 priority 2
 associate ccm 3 priority 3
 associate ccm 4 priority 4
 associate profile 1 register CONF-1
 associate profile 2 register MTP-1
 associate profile 3 register XCODE-1
!
dspfarm profile 3 transcode
 codec g711ulaw
 codec g711alaw
 codec g729ar8
 codec g729abr8
 codec pass-through
 codec g722-64
 codec g729r8
 codec ilbc
 maximum sessions 3
 associate application SCCP
!
dspfarm profile 1 conference
 codec g711ulaw
 codec g711alaw
 codec g729ar8
 codec g729abr8
 codec g729r8
 codec g729br8
 maximum sessions 3
 associate application SCCP
!
```

```
dspfarm profile 2 mtp
 codec g711ulaw
 codec pass-through
 maximum sessions software 110
 associate application SCCP
!
!
```

APPENDIX C

# Configuring Cisco VG224 Analog Voice Gateway

**Revised: June 08, 2010, OL-19142-02**

The example in this appendix illustrates how to configure IPv6 on the Cisco VG224 Analog Voice Gateway.

For additional information on IPv6 configuration, refer to the following documentation:

- *Cisco IOS Voice Command Reference*

  http://www.cisco.com/en/US/docs/ios/voice/command/reference/vr_book.html
- *Cisco IOS IPv6 Command Reference*

  http://www.cisco.com/en/US/docs/ios/ipv6/command/reference/ipv6_book.html

### Cisco VG224 Configuration

```
version 12.4
no service pad
service timestamps debug datetime localtime show-timezone
service timestamps log datetime localtime show-timezone
no service password-encryption
!
hostname vg224-gateway
!
boot-start-marker
boot system slot0:vg224-i6k9s-mz.124-22.T
boot-end-marker
!
ip source-route
ip cef
!
ipv6 unicast-routing
ipv6 cef
!
stcapp ccm-group 1
stcapp
!
voice-card 0
!
archive
 log config
  hidekeys
!
interface FastEthernet0/0
 ip address 101.2.0.4 255.255.255.0
 duplex auto
 speed auto
```

```
 ipv6 address 2001:101:2::4/64
 ipv6 enable
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
router ospf 1
 log-adjacency-changes
 network 101.0.0.0 0.255.255.255 area 0
!
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 101.2.200.1
!
ip http server
no ip http secure-server
!
ipv6 route 2001::/16 2001:101:2::1
ipv6 route ::/0 2001:101:2::1
!
control-plane
!
voice-port 2/0
 timeouts ringing infinity
!
voice-port 2/1
 timeouts ringing infinity
!
voice-port 2/2
 timeouts ringing infinity
!
voice-port 2/3
 timeouts ringing infinity
 shutdown
!
voice-port 2/4
 timeouts ringing infinity
 shutdown
!
voice-port 2/5
 timeouts ringing infinity
 shutdown
!
voice-port 2/6
 timeouts ringing infinity
 shutdown
!
voice-port 2/7
 timeouts ringing infinity
 shutdown
!
voice-port 2/8
 timeouts ringing infinity
 shutdown
!
voice-port 2/9
 timeouts ringing infinity
 shutdown
!
voice-port 2/10
 timeouts ringing infinity
 shutdown
```

```
!
voice-port 2/11
 timeouts ringing infinity
 shutdown
!
voice-port 2/12
 timeouts ringing infinity
 shutdown
!
voice-port 2/13
 timeouts ringing infinity
 shutdown
!
voice-port 2/14
 timeouts ringing infinity
 shutdown
!
voice-port 2/15
 timeouts ringing infinity
 shutdown
!
voice-port 2/16
 timeouts ringing infinity
 shutdown
!
voice-port 2/17
 timeouts ringing infinity
 shutdown
!
voice-port 2/18
 timeouts ringing infinity
 shutdown
!
voice-port 2/19
 timeouts ringing infinity
 shutdown
!
voice-port 2/20
 timeouts ringing infinity
 shutdown
!
voice-port 2/21
 timeouts ringing infinity
 shutdown
!
voice-port 2/22
 timeouts ringing infinity
 shutdown
!
voice-port 2/23
 timeouts ringing infinity
 shutdown
!
ccm-manager fax protocol cisco
!
mgcp fax t38 ecm
!
sccp local FastEthernet0/0
sccp ccm 2001:101:2::11 identifier 3 version 7.0
sccp ccm 2001:101:2::10 identifier 1 version 7.0
sccp
!
sccp ccm group 1
 associate ccm 1 priority 1
```

```
 associate ccm 3 priority 3
!
dial-peer voice 1 pots
 service stcapp
 port 2/0
!
dial-peer voice 2 pots
 service stcapp
 port 2/1
!
dial-peer voice 3 pots
 service stcapp
 port 2/2
!
dial-peer voice 4 pots
 service stcapp
 port 2/3
!
dial-peer voice 5 pots
 service stcapp
 port 2/4
!
dial-peer voice 6 pots
 service stcapp
 port 2/5
!
dial-peer voice 7 pots
 service stcapp
 port 2/6
!
dial-peer voice 8 pots
 service stcapp
 port 2/7
!
dial-peer voice 9 pots
 service stcapp
 port 2/8
!
dial-peer voice 10 pots
 service stcapp
 port 2/9
!
dial-peer voice 11 pots
 service stcapp
 port 2/10
!
dial-peer voice 12 pots
 service stcapp
 port 2/11
!
dial-peer voice 13 pots
 service stcapp
 port 2/12
!
dial-peer voice 14 pots
 service stcapp
 port 2/13
!
dial-peer voice 15 pots
 service stcapp
 port 2/14
!
dial-peer voice 16 pots
 service stcapp
```

```
 port 2/15
!
dial-peer voice 17 pots
 service stcapp
 port 2/16
!
dial-peer voice 18 pots
 service stcapp
 port 2/17
!
dial-peer voice 19 pots
 service stcapp
 port 2/18
!
dial-peer voice 20 pots
 service stcapp
 port 2/19
!
dial-peer voice 21 pots
 service stcapp
 port 2/20
!
dial-peer voice 22 pots
 service stcapp
 port 2/21
!
dial-peer voice 23 pots
 service stcapp
 port 2/22
!
dial-peer voice 24 pots
 service stcapp
 port 2/23
!
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 password lab
 login
!
```

APPENDIX D

# Configuring Cisco IOS Gateways

**Revised: June 08, 2010, OL-19142-02**

The example in this appendix illustrates how to configure Cisco IOS gateways to enable Alternative Network Address Types (ANAT), the ANAT addressing preference, and SIP trunk signaling.

For additional information on IPv6 configuration, refer to the following documentation:

- *Cisco IOS Voice Command Reference*

  http://www.cisco.com/en/US/docs/ios/voice/command/reference/vr_book.html
- *Cisco IOS IPv6 Command Reference*

  http://www.cisco.com/en/US/docs/ios/ipv6/command/reference/ipv6_book.html

### Cisco IOS Gateway Configuration

```
2800-Router(config)#voice service voip
```

Shut down the **voice service voip** to configure dual-stack mode and ANAT preference:

```
2800-Router (conf-voi-serv)#shutdown
2800-Router (conf-voi-serv)#sip-ua

2800-Router (config-sip-ua)#protocol mode dual-stack preference ?
  ipv4  IPv4 address is preferred
  ipv6  IPv6 address is preferred

2800-Router (config-sip-ua)#protocol mode dual-stack preference ipv4
2800-Router (config-sip-ua)#voice service voip
2800-Router (conf-voi-serv)#no shutdown
```

Now the gateway is configured as dual-stack gateway with IPv4 preference.

ANAT is enabled globally by default, but can also be enabled by the following commands:

```
2800-Router (config-sip-ua)#voice service voip
2800-Router (conf-voi-serv)#sip
2800-Router (conf-serv-sip)#anat
```

Use the following command to enable ANAT on each dial-peer:

```
dial-peer voice 1 voip
 description **** SIP Trunk to CUCM ****
 destination-pattern 5...
 voice-class sip anat
 session protocol sipv2
 session target ipv6:[2001:db8:caf0:101:21b:78ff:fe7a:5d86]
```

For signaling, only one destination address can be set, and it should be either IPv4 or IPv6.

```
session transport tcp
dtmf-relay rtp-nte
no vad
```