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

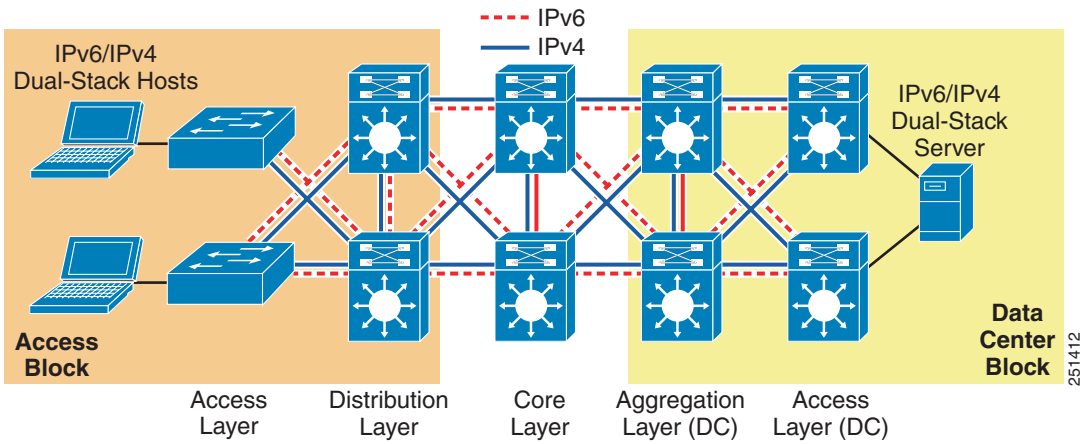
IPv6 multicast routers use Multicast Listener Discovery (MLD) protocol to discover the presence of multicast listeners (nodes wishing to receive IPv6 multicast packets) on its directly attached links and to discover which multicast packets are of interest to neighboring nodes.

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

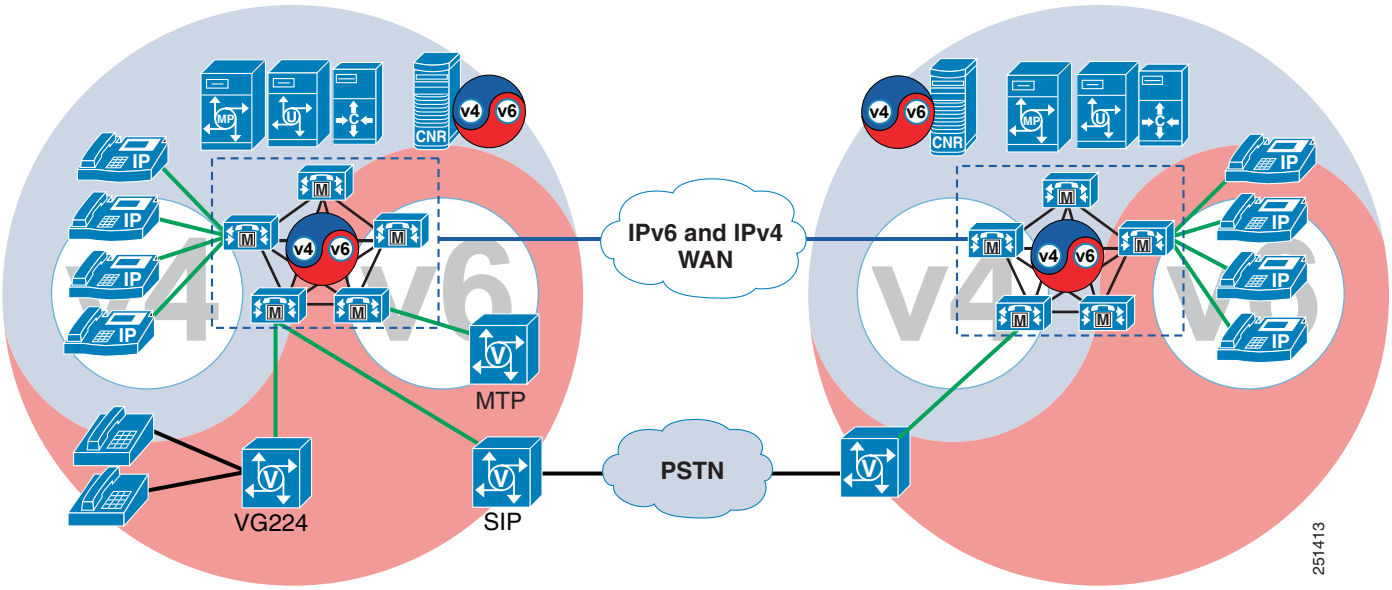
- *Deploying IPv6 in Branch Networks*

  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.

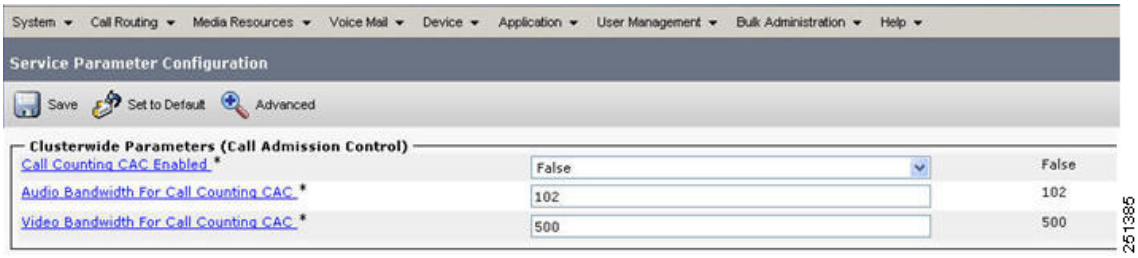
For call-counting call admission control, the following default values are used for Layer 3 voice and video bandwidth when calculating the amount of available bandwidth at a location:

- 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

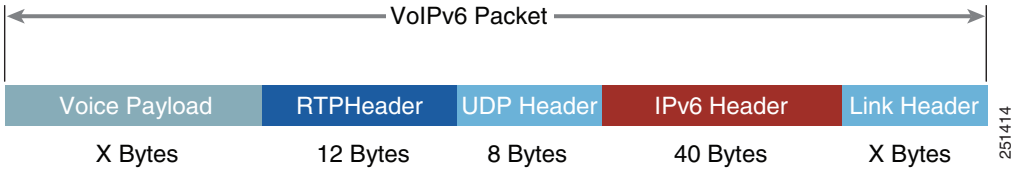
For general recommendations on bandwidth provisioning for Unified Communications traffic, refer to the bandwidth provisioning information in the *Cisco Unified Communications Solution Reference Network Design (SRND)*, available at http://www.cisco.com/go/ucsrnd. However, when provisioning for IPv6 voice 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)