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.

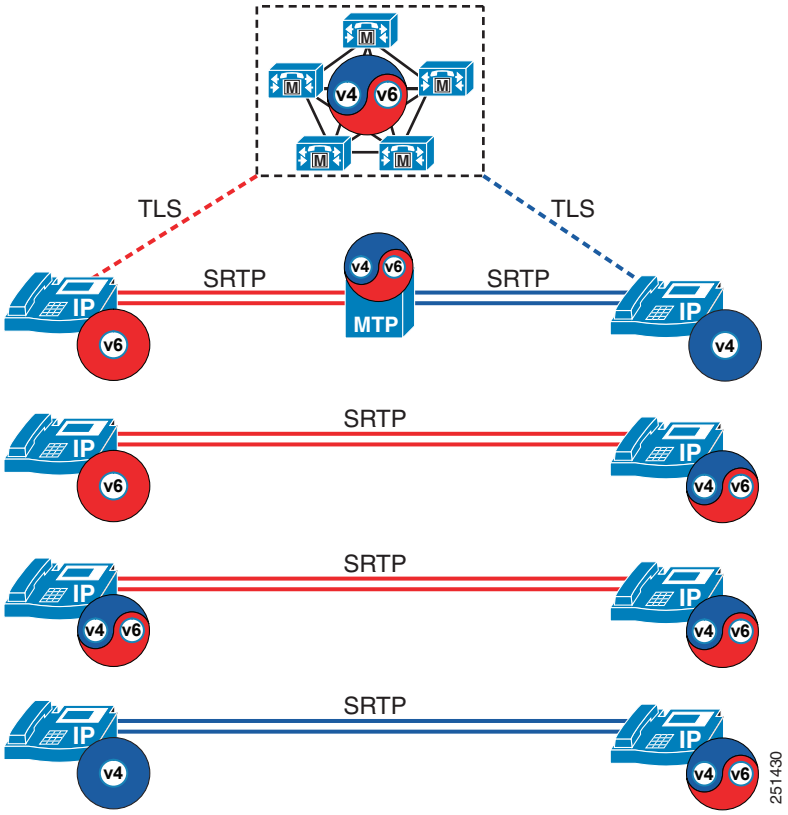
For more information on Unified CM security, refer to the *Cisco Unified Communications Manager Security Guide*, available at

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.