APPENDIX A

Cisco Unified Communications Architecture Basics

This appendix provides a high-level overview of some of the basic architectural concepts and elements upon which the Cisco Unified Communications System is built.

Additional information regarding Voice over IP technologies is available at:

http://www.cisco.com/en/US/tech/tk652/tk701/tsd_technology_support_protocol_home.html

Overview

The Cisco Unified Communications System provides support for the transmission of voice, video, and data over a single, IP-based network, which enables companies to consolidate and streamline communications. The Cisco Unified Communications System is a key part of the Cisco Unified Communications Solution, which also includes network infrastructure, security, and network management products, wireless connectivity, third-party communications applications, and a lifecycle services approach for preparing, planning, designing, implementing, operating and optimizing (PPDIOO) the system.

The Cisco Unified Communications System leverages an existing IP infrastructure (built on the Open System Interconnection [OSI] reference model) and adds support for voice and video-related devices, features, and applications. Support for major signaling protocols, such as the Session Initiation Protocol (SIP), the Media Gateway Control Protocol (MGCP), and H.323 is provided, as is the ability to integrate with legacy voice and video networks.

Table A-1 shows the relationship between the OSI reference model and the voice and video protocols and functions of the Cisco Unified Communications System.

Table A-1 Voice and Video over IP in the OSI Reference Model

OSI Layer Number	OSI Layer Name	Voice	Video
7	Application	Unified IP Phone, Unified Personal Communicator, etc.	Video endpoint, Unified Video Advantage, etc.
6	Presentation	G.711, G.722, G.723, G.729	H.261, H.263, H.264
5	Session	H.323/MGCP/SIP/SCCP	H.323/SIP/SCCP
4	Transport	RTP/UDP, TCP	

OSI Layer Number	OSI Layer Name	Voice	Video
3	Network	IP	
2	Data Link	Frame Relay, ATM, Ethernet, PPP, MLP, and more	

Following this model:

- **Layer 6**—Digital signal processors (DSPs) compress/encode (decompress/decode) the voice or video signal using the chosen codec. The DSP then segments the compressed/encoded signal into frames and stores them into packets.
- **Layer 5**—The packets are transported in compliance with a signaling protocol, such as Skinny Client Control Protocol (SCCP), H.323, MGCP, or SIP.
- **Layer 4**—Signaling traffic (call setup and teardown) uses TCP as its transport medium.

  Media streams use Real-time Transport Protocol (RTP) over UDP for the transport protocol. RTP is used because it inserts timestamps and sequence numbers in each packet to enable synchronization at the receiving end. UDP is used because TCP would introduce delays (due to acknowledgements) that are not easily tolerated by real-time traffic.
- **Layer 3**—The IP layer provides routing and network-level addressing.
- **Layer 2**—The data-link layer protocols control and direct the transmission of the information over the physical medium.

Voice over IP

In general, the components of a VoIP network fall into the following categories:

- Infrastructure—Provides the foundation for the transmission of voice over an IP network. In addition to routers and switches, this includes the interfaces, devices, and features necessary to integrate VoIP devices, legacy PBX, voicemail, and directory systems, and to connect to other VoIP and legacy telephony networks. Typical products used to build the infrastructure include Cisco voice gateways (non-routing, routing, and integrated), Cisco IOS and Catalyst switches, and Cisco routers, as well as security devices, such as firewalls, virtual private networks (VPNs), and intrusion detection systems. In addition, Quality of Service (QoS), high-availability, and bandwidth provisioning (for WAN devices) should be deployed.
- Call processing—Provides signaling and call control services from the time a call is initiated until the time a call is terminated. The call processing component also provides feature services, such as call transfer and forwarding capabilities. In the Cisco Unified Communications System, call processing is performed by Cisco Unified Communications Manager or Communications Manager Express.
- Applications—Includes components that supplement the basic call processing to provide users with a complete suite of communications options. Applications in the Cisco Unified Communications System include Cisco Unity for voice messaging products, Cisco Unified MeetingPlace conference scheduling software, Cisco Emergency Responder, and applications that enhance the usability of the system and allow users to be more productive, such as the Cisco Unified Presence.
- Voice-enabled endpoints—Includes IP phones, soft phones, wireless IP phones, and analog gateways, which provide access to the PSTN and enable interoperability with legacy telephony devices (such as a Plain Old Telephone System [POTS] phone). For IP phones and softphones, the supported protocols are SCCP, H.323, and SIP. For gateways, the supported protocols are SCCP, H.323, SIP, and MGCP.

For a more in depth discussion of Voice over IP, see *Voice over IP Fundamentals* from Cisco Press.

Video over IP

Typical IP videoconferencing components include:

- Gateways—Performs translation between different protocols, audio encoding formats, and video encoding formats that may be used by the various standards. The Cisco Unified Videoconferencing gateways enable conferences using H.323, H.320, SCCP, or SIP endpoints.
- Gatekeepers— Works with the call-processing component to provide management of H.323 endpoints. The gatekeeper handles all Registration, Admission, and Status (RAS) signaling, while the call-processing component handles all of the call signaling and media negotiations.
- Conference bridges—Enables conferencing between three or more participants. Video endpoints are generally point-to-point devices, allowing only two participants per conversation. A conference bridge or multipoint conference unit (MCU) is required to extend a video conference to three or more participants.
- Video-enabled endpoints—Includes stand-alone video terminals, IP phones with integrated video capabilities, and video conferencing software on a PC. These endpoints can be H.323, H.320, SCCP, or SIP.

For additional information about videoconferencing, see the *IP Videoconferencing Solution Reference Network Design* guide.

Fax over IP

Fax over IP enables the interworking of standard fax machines over packet-based networks. With fax over IP, the fax image is extracted from the analog signal and converted to digital data for transmission over the IP network.

The components of the Cisco Unified Communications System support three methods for transmitting fax over IP: real-time fax, store-and-forward fax, fax pass-through.

- For real-time fax, Cisco supports Cisco fax relay and T.38 fax relay (from the International Telecommunications Union [ITU-T]). With this method, the DSP breaks down the fax tones from the sending fax machine into their specific frames (demodulation), transmits the information across the IP network using the fax relay protocol, and then converts the bits back into tones at the far side (modulation). The fax machines on either end send and receive tones as they would over the PSTN and are not aware that information is actually going across an IP network.
- For store-and-forward fax, Cisco supports T.37 (from the ITU-T). With this method, the on-ramp gateway receives a fax from a traditional fax device and converts it into a Tagged Image File Format (TIFF) file attachment. The gateway then creates a standard Multipurpose Internet Mail Extension (MIME) e-mail message and attaches the TIFF file to the e-mail. The gateway forwards the e-mail, now called a fax mail, and its attachment to the messaging infrastructure of a designated Simple Mail Transport Protocol (SMTP) server.

  Store-and-forward fax allows for fax transmissions to be stored and transmitted across a packet-based network in a bulk fashion, which allows faxes to use least-cost routing and enables faxes to be stored and transmitted when toll charges are more favorable. When using store-and-forward fax, however, the user must be willing to accept fax delays that range from seconds to hours, depending upon the particular method of deployment.

- For fax pass-through, fax data is not demodulated or compressed for its transit through the packet network. With this method, the fax traffic is carried between the two gateways in RTP packets using an uncompressed format resembling the G.711 codec. The gateway does not distinguish fax calls from voice calls.

VoIP Protocols

For signaling and call control, the Cisco Unified Communications System supports the Cisco proprietary VoIP protocol, SCCP, as well as the major industry-standard protocols of H.323, SIP, and MGCP. These protocols can be categorized as using either a client-server or peer-to-peer model.

- The *client-server model* is similar to that used in traditional telephony, in which in which dumb endpoints (telephones) are controlled by centralized switches. With a client-server model, the majority of the of the intelligence resides in the centralized call processing component, which handles the switching logic and call control, and with very little processing is done by the phone itself.

  The advantages of the client-server model are that it centralizes management, provisioning, and call control; it simplifies call flows for replicating legacy voice features; it reduces the amount of memory and CPU required on the phone; and it is easier for legacy voice engineers to understand.

  MGCP and SCCP are examples of client-server protocols.

- The *peer-to-peer model* allows network *intelligence* to be distributed between the endpoints and call-control components. Intelligence in this instance refers to call state, calling features, call routing, provisioning, billing, or any other aspect of call handling. The endpoints can be VoIP gateways, IP phones, media servers, or any device that can initiate and terminate a VoIP call.

  The advantages of the peer-to-peer model are that it is more flexible, more scalable, and more easily understood by engineers who are accustomed to running IP data networks.

  SIP and H.323 are examples of peer-to-peer protocols.

Table A-2 Protocols Supported by Cisco Unified Communications Components

Protocol	Description
SCCP	A proprietary protocol from Cisco Systems. SCCP uses the client-server model. Call control is provided by the Cisco Unified Communications Manager or Communications Manager Express. Unified IP Phones run a “skinny” client, which requires very little processing to be done by the phone itself. SCCP is supported by all Cisco IP Phones, by Cisco Unified Video Advantage, by many third-party video endpoints, and by select Cisco gateways.
MGCP	The recommendation from the ITU-T for multimedia communications over LANs. MGCP uses the client-server model and is used primarily to communicate with gateways. MGCP provides easier configuration and centralized management. It is supported by most Cisco gateways.

Protocol	Description
SIP	A recommendation from the Internet Engineering Task Force (IETF) for multimedia communications over LANs. SIP uses the peer-to-peer model. Call control is provided through a SIP proxy or redirect server. In Cisco Unified Communications Manager, SIP call control is provided through a built-in back-to-back user agent (B2BUA). SIP uses a simple messaging scheme and is highly scalable. It is supported by an increasing number of Cisco IP phones, by a number of third-party video endpoints, and on the trunk side of many Cisco gateways.
H.323	The recommendation from the ITU-T for multimedia communications over LANs. H.323 uses the peer-to-peer model. It is based on the Integrated Services Digital Network (ISDN) Q.931 protocol. Call control is provided through a gatekeeper. H.323 provides robust support for interfaces and interoperates easily with PSTN and SS7. It is supported by a number of third-party video endpoints and by most Cisco gateways.

Voice and Video Codecs

As previously mentioned, codecs are used to encode and compress analog streams (such as voice or video) into digital signals that can then be sent across an IP network.

Tip As a general recommendation, if bandwidth permits, it is best use a single codec throughout the campus to minimize the need for transcoding resources, which can add complexity to network design.

Characteristics of a codec are as follows:

- Codecs are either *narrowband* or *wideband*. Narrowband (used by traditional telephony systems) refers to the fact that the audio signals are passed in the range of 300-3500 Hz. With wideband, the audio signals are passed in the range of 50 to 7000 Hz. Therefore, a wideband codec allows for audio with richer tones and better quality.
- The *sampling rate* (or frequency) corresponds to the number of samples taken per second, expressed in Hz or kHz. For digital audio, typical sampling rates are 8 kHz (narrowband), 16 kHz (wideband) and 32 kHz (ultra-wideband). For digital video, typical sampling rates are 50Hz (for Phase-Alternating Line, PAL, used largely in Western Europe) and 59.94 Hz (for National Television System Committee, NTSC, used largely in North America). Both rates are supported by all the video codec listed in Table A-3.
- The *compression ratio* indicates the relative difference between the original size and the compressed size of the audio or video stream. Lower compression ratios yield better quality but require greater bandwidth. In general, low-compression codecs are best suited for voice over LANs and are capable of supporting DTMF and fax. High-compression codecs are better suited for voice over WANs.
- The *complexity* refers to the amount of processing required to perform the compression. Codec complexity affects the call density—the number of calls reconciled on the DSPs. With higher codec complexity, fewer calls can be handled.

The components of the Cisco Unified Communications System support one or more of the audio and video codecs described in Table A-3.

Table A-3 Codecs Supported by Cisco Unified Communications Components

Codec	Description
G.711	A narrowband audio codec defined by the ITU-T that provides toll-quality audio at 64 Kbps. It uses pulse code modulation (PCM) and samples audio at 8 kHz. G.711 supports two companding algorithms; mu-law (used in the US and Japan) and a-law (used in Europe and other parts of the world). G.711 is a low-compression, medium-complexity codec.
G.722	A wideband audio codec defined by the ITU-T that provides high-quality audio at 32 to 64 Kbps. It uses Adaptive Differential PCM (ADPCM) and samples audio at 16 kHz. G.722 is similar to G.711 in compression and complexity, but provides higher quality audio.
G.722.1	A wideband audio codec defined by the ITU-T that provides high-quality audio at 24 and 32 Kbps. It uses Modulated Lapped Transform (MLT) and samples audio at 16 kHz. G.722.1 is a high-compression, low-complexity codec.It provides better quality than G.722 at lower bit-rates.
G.723.1	A narrowband audio codec defined by the ITU-T for videoconferencing that provides near toll-quality audio at 6.3 or 5.3 Kbps. It uses Algebraic Code Excited Linear Prediction (ACELP) and Multi Pulse-Maximum Likelihood Quantization (MP-MLQ) and samples audio at 8 kHz. G.723.1 is a high-compression, high-complexity codec. However, the quality is slightly lower than that of G.711.
G.726	A narrowband codec defined by the ITU-T that provides toll-quality audio at 32 Kbps. It uses ADPCM and samples audio at 8 kHz. G.726 is a medium-complexity codec. It requires half the bandwidth of G.711, while providing nearly the same quality. Note that G.726 supersedes G.723, but has no effect on G.723.1.
G.728	A narrowband codec defined by the ITU-T that provides near toll-quality audio at 16 Kbps. It uses Low Delay CELP (LD-CELP) and samples audio at 8 kHz. G.728 is a high-compression, high-complexity codec.
G.729a	A narrowband audio codec defined by the ITU-T that provides toll-quality audio at 8 Kbps. It uses Conjugate-Structure ACELP (CS-ACELP) and samples audio at 8 kHz. G.729a is a high-compression, medium-complexity codec. The quality is lower than that of G.711 and it is not appropriate for DTMF, but it is good for situations where bandwidth is limited.
iLBC (internet Low Bitrate Codec)	A narrowband audio codec standardized by the IETF that provides better than toll-quality audio at either 13.33 or 15.2 Kbps. It uses block-independent linear-predictive coding (LPC) samples audio at 8 kHz. iLBC provides higher basic quality than G.729 and is royalty free. It enables graceful speech quality degradation in a lossy network. This codec is suitable for real-time communications, streaming audio, archival, and messaging.

Codec	Description
AAC (Advanced Audio Codec)	A wideband audio codec standardized by the Moving Pictures Experts Group (as MPEG-4 AAC). It provides high-quality audio at rates of 32 Kbps and above. It uses AAC-LD (low delay) samples audio at 20 kHz.
L16	A wideband audio codec defined by the IETF as a MIME subtype. It provides reasonable quality audio at 256 Kbps. It is based on PMC and samples audio at 16 kHz.
GSM-FR (Global System for Mobile Communications-Full Rate)	An audio codec defined by the European Telecommunications Standards Institute (ETSI). It was originally designed for GSM digital mobile phone systems and provides somewhat less than toll-quality audio at 13 Kbps. It uses Regular Pulse Excitation with Long-Term Prediction (RPE-LTP) and samples audio at 8 kHz. GSM-FR is a medium-complexity codec.
GSM-EFR (Enhanced Full Rate)	An audio codec defined by the ETSI for digital voice that provides toll-quality audio at 12.2 Kbps. It uses ACELP and samples audio at 8 kHz. GSM-EFR is a high-complexity codec and provides better sound quality than GSM-FR.
QCELP (Qualcomm Code Excited Linear Prediction)	An audio codec defined by the Telecommunications Industry Association (TIA) for wideband spread spectrum digital communication systems that provides toll-quality audio at either 8 or 13 Kbps. As indicated by the name, it uses CELP and samples audio at 8 kHz. QCELP is a high-complexity codec.
H.261	One of the first video codecs defined by the ITU-T. It was originally used for video over ISDN. It is designed to support data rates in multiples of 64 Kbps. H.261 supports Common Intermediate Format (CIF - 352 × 288) and QCIF (176 × 144) resolutions. H.261 is similar to MPEG, however, H.261 requires significantly less computing overhead than MPEG for real-time encoding. Because H.261 uses constant bitrate encoding, it is better suited for use with relatively static video.
H.263	A video codec defined by the ITU-T as an improvement to H.261. It is used in H.323, H.320, and SIP networks. In addition to CIF and QCIF, H.263 supports SQCIF (128 x 96), 4CIF (704 x 576), and 16CIF (1408 x 1152) resolutions. H.263 provides lower bitrate communication, better performance, and improved error recovery. It uses half pixel precision and variable bitrate encoding, which makes H.263 better suited to accommodate motion in video.
H.264	The next in the evolution of video codecs. It was defined by the ITU-T in conjunction with the MPEG (as MPEG-4 Part 10) and is designed to provide higher-quality video at lower bit rates. H.264 provides better video quality, compression efficiency, and resilience to packet and data loss than that of H.263. It also makes better use of bandwidth, resulting in the ability to run more channels over existing systems.

Voice- and Video-enabled Infrastructure

By default, an IP data network transmits data based on the concept of "best effort." Depending on the volume of traffic and the bandwidth available, data networks can often experience delays. However, these delays are typically a matter of seconds (or fractions of seconds) and go unnoticed by users and applications, such as e-mail or file transfers. In the event of significant network congestion or minor route outages, receiving devices can wait and reorder any out-of-sequence packets and sending devices can simply resend any dropped packets.

Voice and video are very time-dependant media, which suffer greatly when subjected to the delays that data applications easily tolerate. In the event of significant congestion or outages, voice applications can only attempt to *conceal* dropped packets, often resulting in poor quality. Therefore, voice and video require an infrastructure that provides for smooth, guarenteed delivery.

A network infrastructure that transmits voice and video, especially that delivered in real-time, requires special mechanisms and technologies to ensure the safety and quality of the media as well as the efficient use of the network resources. In a voice- or video-enabled network, the following must be built into the infrastructure:

- Quality of service
- High availability
- Voice security
- Multicast capabilities

Quality of Service

Quality of Service (QoS) is defined as the measure of performance for a transmission system that reflects its transmission quality and service availability. The transmission quality of the network is determined by the following factors:

- Loss—Also known as packet loss, is a measure of packets faithfully transmitted and received compared to the total number that were transmitted. Loss is expressed as the percentage of packets that were dropped.

  Loss is typically a function of availability (see the "High Availability" section on page A-10). If the network is Highly Available, then loss (during periods of non-congestion) would essentially be zero. During periods of congestion, however, QoS mechanisms can be employed to selectively determine which packets are more suitable to be dropped.

- Delay—Also known as latency, is the finite amount of time it takes a packet to reach the receiving endpoint after being transmitted from the sending endpoint. In the case of voice, this equates to the amount of time it takes for sounds to leave the speaker's mouth and be heard in the listener's ear. This time period is termed the "end-to-end delay."

  There are three types of delay:

  - Packetization delay—The time required to sample and encode analog voice signals and digitize them into packets.
  - Serialization delay—The time required to place the packet bits onto the physical media.
  - Propagation delay—The time required to transmit the packet bits across the physical media.

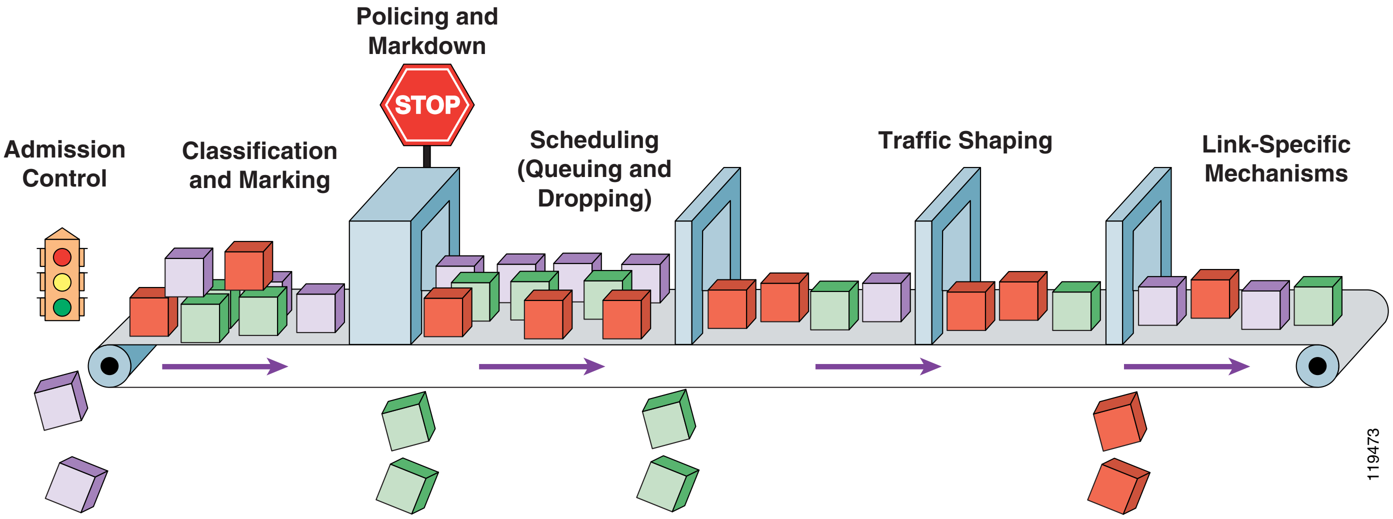
- Delay Variation—Also known as interpacket delay, is the difference in the end-to-end delay between packets. For example, if one packet required 100 ms to traverse the network from the source-endpoint to the destination-endpoint and the following packet required 125 ms to make the same trip, then the delay variation would be calculated as 25 ms.

  Each end station in a VoIP or Video over IP conversation has a jitter buffer. Jitter buffers are used to smooth out changes in arrival times of data packets containing voice. A jitter buffer is dynamic and adaptive, and can adjust for up to a 30 ms average change in arrival times of packets. If you have instantaneous changes in arrival times of packets that are outside of the capabilities of a jitter buffer's ability to compensate you will have jitter buffer over-runs and under-runs.

  - A jitter buffer under-run occurs when the arrival times of packets increases to the point where the jitter buffer has been exhausted and contains no packets to be processed by the DSPs when it is time to play out the next piece of voice or video.
  - A jitter buffer over-run occurs when packets containing voice or video arrive faster than the jitter buffer can dynamically resize itself to accommodate. When this happens, packets are dropped when it is time to play out the voice or video samples, resulting in degraded voice quality.

Cisco provides a QoS toolset that allows network administrators to minimize the effects of loss, delay, and delay variation. These tools (as shown in Figure A-1) enable the classification, scheduling, policing and shaping of traffic—the goal being to give preferential treatment to voice and video traffic.

Figure A-1 Cisco QoS Toolkit



- *Classification* tools mark a frame or packet with a specific value. This marking (or remarking) establishes a trust boundary on which the scheduling tools depend.
- *Scheduling* tools determine how a traffic exits a device. Whenever traffic enters a device faster than it can exit it (as with speed mismatches), then a point of congestion develops. Scheduling tools use various buffers to allow higher-priority traffic to exit sooner than lower priority traffic. This behavior is controlled by queueing algorithms, which are activated only when a devices is experiencing congestion and are deactivated when the congestion clears.

- *Policers* and *shapers* are the oldest forms of QoS mechanisms. These tools have the same objectives—to identify and respond to traffic violations. Policers and shapers identify traffic violations in an identical manner; however, they respond differently to these violations. A policer typically drops traffic; a shaper typically delays the excess traffic using a buffer to hold packets and shape the flow when the data rate of the source is higher than expected.

For more information about QoS considerations and tools, see the Enterprise QoS Solution Reference Network Design Guide.

High Availability

The objective of high availability is to prevent or minimize network outages. This is particularly important in networks that carry voice and video. More than a single technology, high availability is an approach to implementing a mixture of policies, technologies, and inter-related tools to ensure end-to-end availability for services, clients, and sessions. High availability heavily on network redundancy and software availability.

Network redundancy depends on redundant hardware, processors, line cards, and links. The network should be designed so that it has no single points of failure for critical hardware (for example, core switches). Hardware elements, such as cards, should be "hot swappable," meaning they can be replaced without causing disruption to the network. Power supplies and sources should also be redundant.

Software availability depends on reliability-based protocols, such as Spanning Tree and Hot Standby Routing Protocol (HSRP). Spanning Tree, HSRP, and other protocols provide instructions to the network and/or to components of the network on how to behave in the event of a failure. Failure in this case could be a power outage, a hardware failure, or a disconnected cable. These protocols provide rules to reroute packets and reconfigure paths. The speed at which these rules are applied is called convergence. A converged network is one that, from a user standpoint, has recovered from a failure and can now process instructions and/or requests.

For more information about high availability, see *Campus Network for High Availability Design Guide*.

Security

As with important data traffic, voice (and often video) traffic on an IP network must be secured. In some cases, the same technologies that can be used to secure a data network are employed in a VoIP network. In other cases, unique technologies must be implemented. In both cases, one of the key objectives is to protect the voice or video stream without impacting the quality.

When securing the network, it is important to consider all possible areas of vulnerability. This means protecting the network from internal and external threats, securing internal and remote connectivity, and limiting network access to devices, applications, and users that can be trusted. Comprehensive security is achieved first by securing the network itself, and then by extending that security to endpoints and applications. For voice and video communications, security must protect four critical elements:

- Network infrastructure—The switches, routers, and connecting links comprising the foundation network that carries all IP data, voice, and video traffic. This includes using tools such as:
  - Firewalls
  - Network intrusion detection and prevention systems
  - Voice- and video-enabled VPNs
  - VLAN segmentation
  - Port security

- Access control server/user authentication and authorization
- Dynamic Address Resolution Protocol (ARP) inspection
- IP source guard and Dynamic Host Configuration Protocol (DHCP) snooping
- Wireless security technologies, such as wired equivalent privacy (WEP) and Lightweight Extensible Authentication Protocol (LEAP)

- Call processing systems—Servers and associated equipment for call management, control, and accounting. This includes using tools such as:
  - Digital certificates
  - Signed software images
- Endpoints—IP phones, soft phones, video terminals, and other devices that connect to the IP Communications network. This includes using tools such as:
  - Digital certificates
  - Endpoint authentication
  - Secure RTP stream encryption
  - Switch port security
  - Virus protection and integrated Cisco Security Agent
- Applications—User applications such as unified messaging, conferencing, customer contact, and custom tools that extend the capabilities of IP Communications systems. This includes using tools such as:
  - Secure management
  - Multilevel administration
  - Media encryption
  - Use of H.323 and SIP signaling
  - Hardened platform
  - Virus protection and integrated Cisco Security Agent

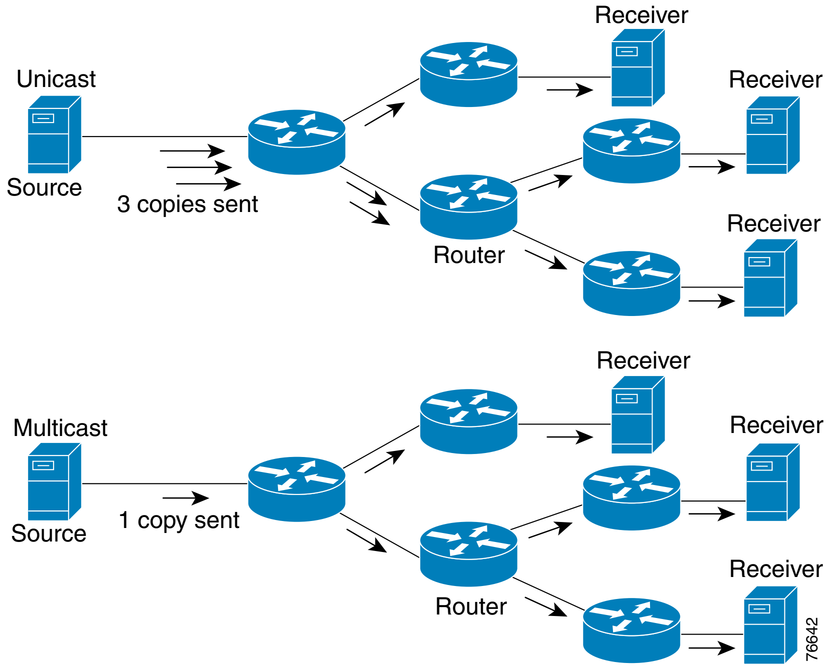
IP Multicast

IP multicast allows for a streamlined approach to delivering data to multiple hosts that need to receive the same data at the same time, such as with distance learning. With IP multicast, an audio or video stream can be sent from a single server to multiple endpoints. For example:

- When configured for IP multicast services, Music-on-Hold (MoH) can stream the same audio file to multiple IP phones without the overhead of duplicating that stream one time for each phone on hold.
- IP/TV allows for the streaming of audio, video, and slides to thousands of receivers simultaneously across the network. High-rate IP/TV streams that would normally congest a low-speed WAN link can be filtered to remain on the local campus network.

In contrast to unicast, which would send individual streams to each of the recipients, IP multicast simultaneously delivers a *single stream* of information to thousands of recipients, thereby reducing bandwidth consumption, as shown in Figure A-2.

Figure A-2 IP Multicast



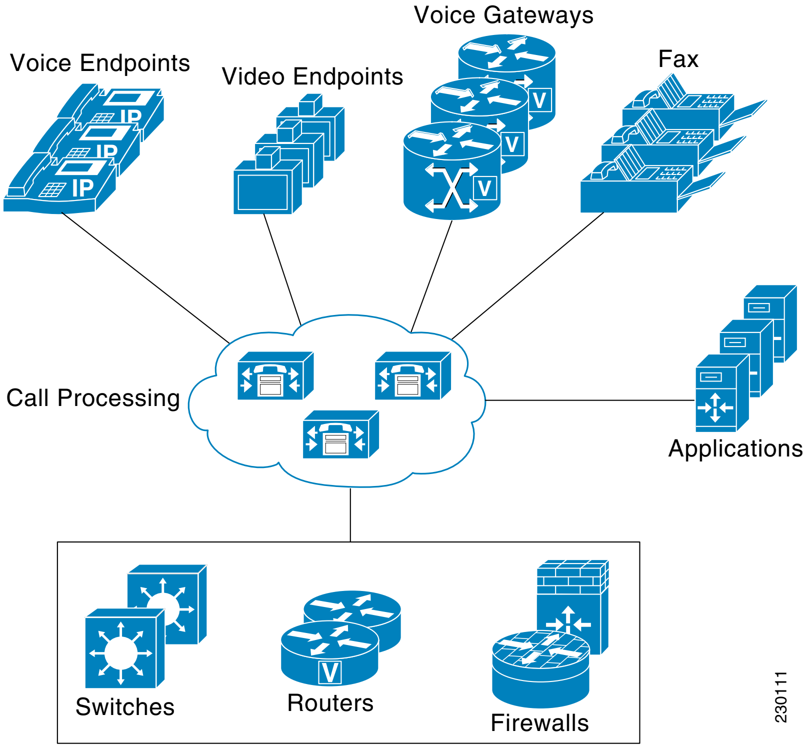
Multicast packets are replicated in the network by Cisco routers and switches enabled with Protocol Independent Multicast (PIM) and other supporting multicast protocols. These routers create “distribution trees,” which control the path that IP Multicast traffic takes through the network in order to deliver traffic to all the receivers.

For more information about IP multicast, see the Cisco Avvid Network Infrastructure IP Multicast Design Guide.

Summary

The components and technologies of the Cisco Unified Communications System and the enabling infrastructure work in concert to deliver converged voice, video, and data communications.

Figure A-3 Cisco Unified Communications System



- The components and technologies employed in the infrastructure (such as QoS and IP Multicast) provide a secure, robust, reliable, and efficient foundation.
- Building on the infrastructure, the gateways and call-processing components perform the necessary conversion, integration, and control functions to enable efficient, streamlined communications.
- The applications augment the call processing to provide features an services required by users.
- And the endpoints provide access to the network services and features—enabling users to make the most of their communications system and increase their productivity.