Cisco Systems

White Paper

SAFE:
IP Telephony Security in Depth

Author

Jason Halpern is the primary author of this white paper and the lead architect for the reference implementation at Cisco Systems headquarters in San Jose, CA USA. Jason is a network architect focused on VPN and security issues.

Abstract

This paper provides best-practice information to interested parties for designing and implementing secure IP telephony networks.utilizing elements of the SAFE blueprints. All SAFE white papers are available at the SAFE Web site: http://www.cisco.com/go/safe. These documents were written to provide best-practice information on network security and virtual-private-network (VPN) designs. Although you can read this document without having read either of the two primary security design documents, it is recommended that you read either “SAFE Enterprise” or “SAFE Small, Midsize and Remote-User Networks” before continuing. This paper frames the IP telephony implementation within the context of the overall security design. SAFE represents a system-based approach to security and VPN design. This type of approach focuses on overall design goals and translates those goals into specific configurations and topologies. In the context of IP telephony, Cisco recommends that you also consider network design elements such as QoS and resiliency when deciding on an overall IP telephony design. SAFE is based on Cisco products and those of its partners.

This document begins with an overview of the architecture, and then details the specific designs under consideration. The following designs are covered in detail:

- Small-network IP telephony
- Medium-network IP telephony
- Large-network IP telephony

Within each design multiple modules may address different aspects of IP telephony technology. The concept of modules is addressed in the SAFE security white papers. Topics covered in each design or module (where appropriate) include:

- Overall design best practices
- Access control and packet inspection
- Performance and scalability
- High Availability
- Secure Management
- Alternatives for the design

Following the discussion of the specific designs, Appendix A details the validation lab for SAFE IP telephony and includes configuration snapshots. Appendix B is a primer on IP telephony. Readers who are unfamiliar with basic IP telephony concepts are encouraged to read this section first. Appendix C contains glossary definitions of the technical terms used in this document.

Audience

This document is intended for either the datacom or telecom network manager. Though this document is technical, it can be read at different levels of detail, depending on the reader. A network manager, for example, can read the introductory sections in each area to obtain a good overview of IP telephony design strategies and considerations. A network engineer or designer can read this document in its entirety and gain design information and threat analysis details, which are supported by actual configuration snapshots for the devices involved. Because this document covers a wide range of IP telephony deployments, it may be helpful to read the introductory sections of the paper first and then skip right to the type of IP telephony network you are interested in deploying.

Caveats

This document presumes that you already have a security policy in place. Cisco Systems does not recommend deploying any technology without an associated security policy. It presumes you are aware of what data is sensitive in your network so that it can be properly protected when transported throughout the network. Although the topic of data network security is mentioned in this document, it is not described in great detail. Security within this document is always mentioned as it pertains to IP telephony technology and the voice network. Readers interested in more information on data network security should look to the SAFE security documents for detailed design guidance.

Following the guidelines in this document does not guarantee a secure environment, or that you will prevent all penetrations. It is the intention of the author to provide you with enough information such that you will make an informed choice as to the risks and benefits that the technology holds. Only after you have weighed the risks and benefits should you deploy any technology. You can achieve reasonable security by establishing a good security policy, following the guidelines in this and the SAFE security documents, staying up-to-date on the latest developments in the hacker and security communities, and maintaining and monitoring all systems with sound system administration practices. This paper attempts to build “secure” IP telephony networks. However it should be noted that today there are no widely adopted protocols for call control or voice transport that support integrated security features such as confidentiality and strong authentication. Thus until the standards progress and are widely adopted we will rely on securing the surrounding network and its components.

Though this document contains a large amount of detail on many aspects of IP telephony technologies, the discussion is not exhaustive. In particular, several technologies that relate to IP telephony are not covered; for example, the security of voice protocols between voice gateways is not addressed. This document focuses on the security of voice as it relates to the Internet Protocol (IP), not legacy systems. Another topic not discussed is best practices for implementing quality of service (QoS) in IP telephony-enabled networks. A viable IP telephony-enabled network requires implementation of QoS throughout the infrastructure; however, discussion of such implementation is out of the scope of this document. If the network does not support QoS, do not attempt to add IP telephony. Using IP Security (IPSec) virtual private networks (VPNs) to provide secure transport for IP telephony is another topic not covered in this document. For this reason the SAFE VPN-centric remote designs are not covered. This document addresses centralized but not distributed call processing. It is assumed that all remote sites have a redundant link to the headend or local call-processing backup in case of headend failure. Finally, the interaction between Network Address Translation (NAT) and IP telephony for the most part is not addressed. It is assumed that all networks are private in order to guarantee QoS, in which case nonoverlapping address ranges should be used. It is assumed that all networks are privately addressed and do not contain overlapping IP addresses.

Architecture Overview

Design Fundamentals

SAFE IP telephony emulates as closely as possible the functional requirements of today's networks. Implementation decisions varied, depending on the network functionality required. However, the following design objectives, listed in order of priority, guided the decision-making process.

- Security and attack mitigation based on policy
- Quality of service
- Reliability, performance, and scalability
- Authentication of users and devices (identity)
- Options for high availability (some designs)
- Secure management

First and foremost, SAFE IP telephony must provide ubiquitous IP telephony services to the locations and users that require it. It must maintain as many of the characteristics of traditional telephony as possible while doing so in a secure manner. Finally, it must integrate with existing network designs based on the SAFE security architecture and not interfere with existing functions.

The term "call-processing manager" is used throughout this document. Some readers may be more familiar with the term "IP PBX." The term "voice-mail system" is used to refer to an IP-based voice-mail storage device.

The State of IP Telephony

Numerous threats, from device failures to malicious attacks, affect the uptime of networks. With the reliance on the IP network for telephony, IP-based threats must be mitigated. In comparison to the traditional data segment, we must guarantee the ability for hundreds, perhaps thousands, of IP phones to dial emergency services (e.g. 911) in case of emergency at any time. This paper covers the techniques that exist today to mitigate these attacks, providing best practices for all IP telephony systems. However, as previously mentioned there is no widely adopted and deployed standard today for IP telephony call control, nor for delivery of features to IP phones or PC-based IP Phones. Most vendors today rely on proprietary control protocols. For instance, Cisco uses the Skinny Station Protocol for call control. Because of this the provided best practices may not be applicable in all IP telephony environments.

SAFE IP Telephony Axioms

The following axioms represent overarching design considerations that affect nearly every design within SAFE IP telephony. They are included in the front of this document to limit the amount of redundancy in the rest of the paper. SAFE IP telephony assumes conformance with the security axioms in the original SAFE white paper. Although IP telephony design differs greatly with the size of enterprises, the underlying best practices remain virtually the same. For this reason the design discussions are somewhat similar. In the axioms it is assumed that the users and sites are members of your enterprise and in your domain of control.

Voice Networks Are Targets

Voice networks are juicy targets for hackers with ulterior motives. Some may want to play a prank by sending a voice-mail to every member of your company claiming to be a Human Resource (HR) representative telling them to take the day off. Others would be happy with accessing your Chief Financial Officer's (CFO's) voice-message box a week before your company's earnings were due on Wall Street. Further still, imagine the damage a hacker could do eavesdropping on phone conversations with your customers or better yet forwarding the calls you had with them to your competitors. We haven't seen these types of attacks documented yet in IP voice networks but we have seen very similar attacks to these in IP data networks. The main issue with voice networks today is that they are generally wide open and require little or no authentication to gain access. The reason for this is that the model chosen for IP voice networks parallels that chosen for legacy voice systems. Our expectation going forward is that traditional security featrures such as strong authentication and encryption will integrate with IP telephony standards. Regardless of the future need for a standards-based and integrated approach to secure IP telephony, we can effectively use a number of existing data-centric security technologies for increased voice security today.

Data and Voice Segmentation Is Key

IP-based telephony provides a means of providing telephony over the existing IP data network. However, for reasons including QoS, scalability, manageability, and security, deployment of IP telephony devices and IP data devices should occur on two logically disparate segments. Segmenting IP voice from the traditional IP data network greatly increases attack mitigation capability and allows use of the same access, core, and distribution layers.

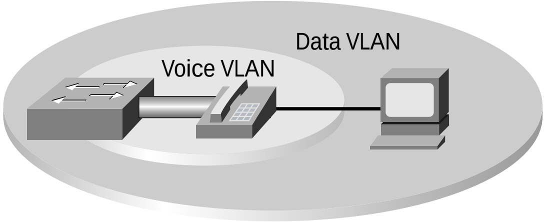
Although the segments should be disparate, Cisco by no means recommends deploying two IP infrastructures. Technologies such as virtual LANs (VLANs), access control, and stateful firewall, provide the Layer 3 segmentation necessary to keep the voice and data segments separate at the access layer.

Telephony Devices Don't Support Confidentiality

The combination of data and voice segmentation and a switched infrastructure strongly mitigates call eavesdropping attacks. For instance, the tool "voice over misconfigured Internet telephones" (also known as vomit), takes an IP phone conversation trace captured by the UNIX tool tcpdump, and reassembles it into a wave file for easy listening. The phones are not actually misconfigured. Rather, if someone was able to obtain access to the IP data stream at any point in the network they could eavesdrop. To a degree keeping the segments separate thwarts devices in the data segment from listening to calls in the voice segment. An obvious way arround this segmentation is to unplug an IP phone in the voice segment and plug in another device such as a workstation. Using a switched infrastructure by definition should thwart a device even in the same segment from call monitoring. However, tools such as dsniff effictively turn the switched medium into a shared medium. Thus segmentation provides minimal attack mitigation by itself. The true value of segmentation is the ability to tune network intrusion detection systems (NIDSs) as outlined in the *secure and monitor all voice servers and segments* axiom.

One additional attack should also be noted. If the hacker has access to the local switched segment, the hacker might be able to insert a phone into the voice segment with a spoofed Media Access Control (MAC) address, assume the target phone's identity, and intercept a call. Mitigation techniques for this attack are discussed in the following rogue devices axiom.

Figure 1
IP phone data and voice VLAN segmentation



IP Phones Provide Access To The Data-Voice Segments

Many IP phones support a data port to allow the connection of a PC to the phone so that only a single cable is necessary to provide data and voice connectivity to the user's workspace. When this occurs follow the data/voice segmentation principle. Some IP phones only provide basic Layer 2 connectivity. Meaning the IP phone essentially acts as a hub combining the data and voice segments. Some IP phones provide enhanced Layer 2 connectivity with the option to use VLAN technology, such as 802.1q, to place the phone and the data port in two different VLANs. This architecture assumes that the IP phones deployed, support VLANs to keep the data and voice segments separate. As discussed in the original SAFE paper, security designs should not rely solely on VLANs for network separation. Rather, they should follow layered security best practices and also rely on Layer 3 access control in the distribution layer into which the IP phone connects. This best practice is followed in all designs.

PC-based IP Phones Require Open Access

Because the deployment of PC-based IP Phones provides a path for attacks against the voice segment, we don't recommend their usage unless a stateful firewall brokers the data-voice interaction. PC-based IP Phones by their nature reside in the data segment and require access to the voice segment in order to access call control, place calls to IP phones, and leave voice messages. Calls placed between IP telephony devices generally use dynamically assigned User Datagram Protocol (UDP) port numbers greater than 16384, thus requiring a stateful inspection device to allow pinpoint access between the segments. Without a stateful firewall brokering all connections between the data and voice networks, you would have to allow wide UDP port ranges. In most networks it will not be possible to secure all connections between the data and voice segments with a stateful firewall. Consider that in an enterprise multiple data and voice segments will exist, most likely on the same switch. Here stateful firewall segmentation would not be feasible, nor would Layer 3 stateless filtering suffice.

Without a stateful firewall present a UDP flood denial-of-service (DoS) attack launched from the data segment could easily overwhelm the voice segment. For this reason Cisco does not recommend placing IP telephony-capable devices on the data segment unless a stateful firewall is present. Regardless of this recommendation, this paper discusses other issues relating to PC-based IP Phones as they may be deployable in some environments and it is important to understand all the issues at hand.

PC-based IP Phones Are Especially Susceptible To Attacks

PC-based IP Phones are not as resilient under attack as their IP phone counterparts. In comparison, PC-based IP Phone hosts are more susceptible to attacks due to the number of vectors into the system. These include Operating System (OS) vulnerabilities, application vulnerabilities, service vulnerabilities, worms, viruses, etc. IP phones run custom OSs with limited service support and are less likely to have vulnerabilities. Another issue is that because the PC-based IP Phone resides in the data segment, it is susceptible to any attack against that entire segment and not just the host itself. The Code-Red and Nimda worms/viruses, for instance, bogged down PC-based IP Phone user systems and the segments they resided in to such a point that they were unusable. No amount of QoS will prioritize voice traffic over data traffic in the data segment if the end system placing the call is unusable.

Controlling the Voice-to-Data Segment Interaction Is Key

Only by methodically controlling access between the data and voice segments is it possible to deploy a secured IP telephony network. To accomplish this task use a stateful firewall since it provides host-based DoS protection against connection starvation and fragmentation attacks, dynamic per-port-granular access through the firewall when legitimate and necessary, spoof mitigation, and general filtering. All designs in this paper follow this best practice. As discussed previously with regards to PC-based IP Phones, we are not advocating placing a stateful firewall between all segments. Rather, we require a stateful firewall at specific locations in the network where the segments are allowed to interact. Anywhere else in the network no communication between the segments is allowed and to carry this out stateless Layer 3 filtering is sufficient. There are multiple legitimate flows between the data and voice segments that should be allowed and we will discuss each flows' requirements and security issues. In general, the firewall will broker the following connections:

- *The voice-mail system when placed in the data segment connecting to the call-processing manager in the voice segment*—Unified voice-mail systems use the traditional e-mail store in the data segment for voice-message storage and require communication with the call-processing manager to notify users of voice mail. Generally this service runs over well-known TCP ports. The firewall mitigates connection starvation DoS and protocol attacks against the call-processing manager. The voice-mail system may reside in the data or voice segments depending on the scalability requirements and the location of the existing e-mail system if unified messaging is deployed.
- *IP phones in a voice segment connecting to the call-processing manager in another voice segment for call establishment control and configuration.* Generally these services run over a combination of well-known TCP ports and UDP. The firewall mitigates connection starvation DoS and protocol attacks against the call-processing manager. It also opens port-level-granular access for UDP between the segments. To mitigate attacks it is reccomended that the call-process manager and IP phones reside in seperate voice segments; this is normally done for increased scalability and ease of management.
- *IP phones in the voice segment connecting to the voice-mail system when placed in the data segment*—Users need to be able to leave voice messages on the voice-mail server not only locally, but also remotely in the case of branch offices. The firewall opens port-level-granular access for UDP between the segments and mitigates general DoS attacks against the IP phones.
- *IP phones in the voice segment browsing resources via the proxy server in the voice segment*—This might include employee user directories or even Internet access for news. Generally this service runs over well-known TCP ports. The firewall mitigates connection starvation DoS and protocol attacks against the proxy server.
- *Users in the data segment browsing the call-processing manager in the voice segment*—IP phone users will need to be able to modify custom configuration settings of their phone. Generally this service runs over well-known TCP ports. The firewall mitigates connection starvation DoS and protocol attacks against the call-processing manager.
- *Proxy server in the voice segment accessing resources in the data segment*—The server proxies all requests by the IP phone services. Generally these services run over well-known TCP ports. The firewall mitigates connection starvation DoS and protocol attacks against the proxy server.

The following two connections will exist only if PC-based IP Phones are deployed:

- PC-based IP Phone in the data segment accessing the call-processing manager in the voice segment for call establishment. Generally this service runs over well-known TCP ports. The firewall mitigates connection starvation DoS and protocol attacks against the call-processing manager.
- PC-based IP Phones in the data segment accessing the voice-mail system when placed in the voice segment, (this may not be possible in many networks as discussed previously)—Users need to be able to leave voice messages on the voice-mail server not only locally, but also remotely in the case of branch offices. The firewall opens port-level-granular access for UDP between the segments and mitigates general DoS attacks against the voice-mail system.

Use private address space for all IP telephony devices, namely that provided by RFC 1918, to reduce the likelihood that traffic could traverse outside of your network. This provides the added benefit that hackers outside of your network will not be able to scan the voice segment for vulnerabilities unless NAT is misconfigured. If possible, use different RFC 1918 address space in the data and voice segments to facilitate filtering and recognition. Although stateful firewalls are used in all of the designs to front end the call-processing manager, NAT is not in effect for traffic routed within the voice segments. NAT is used between the data and voice segments in all designs to support IP phone services via the proxy server. All Layer 3 devices mitigate voice segment IP address spoofing via filtering as outlined in RFC 2827.

Establishing Identity Is Key

Whenever possible use user and device authentication as this mitigates many attacks against the IP telephony network. The primary method for the device authentication of IP phones is the MAC address. If a phone with an unknown MAC address attempts to download a network configuration from the call-processing manager, and it has no knowledge of the IP phone's MAC address, then that IP phone will not receive a configuration assuming automatic registration has been disabled. This setup prevents someone from placing a rogue phone into the network and then placing a call, unless of course the person spoofs the MAC address in hopes of intercepting calls; additional mitigation for this attack is discussed in the next section. Some IP phones support basic user authentication, which provides a facility for a user to "log in" onto a phone. By providing either a valid password or personal ID number (PIN), the attacker is granted access to the phone and a custom configuration. User authentication occurs after successful device authentication. This feature was originally designed for shared office spaces and may be an inconvenience for the everyday office worker. Some IP telephony systems also support legacy features such as requiring a user to enter an access code before placing calls to restricted locations. Typically these codes are fixed, changed infrequently, and are sent over the IP network in the clear.

User authentication mitigates more effectively attacks in which a device spoofs a MAC address and attempts to assume the identity of its target. Requiring user authentication also provides some level of nonrepudiation in that if both parties are successfully authenticated, it provides some level of certainty that you can trust the party on the other side of the call. Of course if the user walks away from their desk without logging out, all bets are off. Enable call control logging on the call-processing manager to provide records of placed calls as this aids in nonrepudiation. Some PC-based IP Phones provide Windows-based authentication while others use a username/password/PIN combination. In any case where PINs or passwords are used, they should be aged and changed frequently.

A username/password/PIN combination may also be used to identify the user to the call-processing manager. This feature allows users to access their custom configuration settings after successfully authenticating and is recommended. Even further still, some voice-mail systems support two-factor authentication. In this scenario, users must undergo strong authentication in order to change their custom settings (for example, greeting message) or to listen to voice mail. We do nott recommend deploying this feature unless the sensitivity of the voice messages mandates it.

Rogue Devices Pose Serious Threats

Locking down the switched ports, segments, and services in the network will provide attack mitigation for rogue devices. As in any IP network, there is value in mitigating the capabilities of a rogue device plugged into the network. As the original SAFE papers addressed, these include best practices such as disabling unused ports and deploying a switched environment. All of these best practices also hold true in the voice segment, but some additional steps should be taken. The following four best practices provide mitigation details specific to IP telephony.

First, since Dynamic Host Configuration Protocol (DHCP) is typically used for a scalable IP phone deployment, consider statically assigning IP addresses to known MAC addresses. This way, the IP phone always has the same address, and if an unknown device is plugged into the network, it does not receive an address. Though a hacker could still statically assign both an IP and MAC address on a device to subvert this practice, doing so is not easy and will thwart most basic attacks. In case automatic registration is left enabled on the call-processing manager, with this practice in place it is less likely that a device could register on the network. It also provides migration against the following DHCP DoS attack. By using separate DHCP servers for the voice and data segments, a DoS launched against the DHCP server in the data segment would not interfere with IP phone address allocation in the voice segment. Fixing IP address allocation to known MAC addresses greatly reduces the likelihood of a successful IP address DoS starvation attack against the voice DHCP server. Many enterprises may find this technique difficult to put into effect however it is provided here so that you can consider its pros and cons.

Second, many call-processing managers provide an automatic phone registration feature that bootstraps an unknown phone with a temporary configuration and then allows it to interact with the network. Turn this functionality off for normal day-to-day use. You should only use it temporarily for bulk deployment of phones. Configure the call-processing manager to deny unknown PC-based IP Phone access. This will provide mitigation for unknown devices that should not be allowed to utilize the call-processing manager to register on the network.

Third, consider using a utility such as Arpwatch to monitor the MAC addresses in your voice segment. In comparison to the data segment, MAC addresses are more likely to be static and Arpwatch will track the MAC addresses of all devices in the voice segments. Arpwatch logs any changes in MAC to IP address pairings. For more information on Arpwatch refer to http://www-nrg.ee.lbl.gov/nrg.html.

Finally, filtering in all segments should limit devices in unknown segments from connecting to the call-processing manager. If a rogue device is placed in a segment not approved for IP telephony use, filtering should prevent the device from registering on the network via the call-processing manager. If a rogue call-processing manager is placed in the network, filtering should prevent the redirection of IP telephony devices to it. If a rogue voice gateway is placed in the network, filtering should not allow it to connect to the call-processing manager. In conclusion, All of the above techniques covered in this axiom will help to mitigate toll fraud by not allowing unknown devices to gain access to the call-processing manager.

Secure and Monitor All Voice Servers And Segments

It is no surprise that the same attacks that have the potential to cripple key production servers in the data segment can also have the same effect on the voice servers in the voice segment. For this reason, many of the same precautions should be taken. NIDSs are a powerful tool that should be used to alarm, log, and in some cases react to attack signatures detected in the network. Today, NIDS does not provide voice control protocol attack signatures. It does however provide signatures for UDP DoS attacks and Hypertext Transfer Protocol (HTTP) exploits that are applicable in voice environments. Deploy NIDS in front of the call-processing manager to detect attacks sourced from the data segment against its HTTP user service. Deploy NIDS between the voice and data segments in order to detect DoS attacks against the voice segment.

As mentioned previously with regards to firewalls, providing stateful firewall functionality between the voice and data segments will be difficult for most enterprises. However NIDS, unlike a firewall, is supported in switches today and makes the feasibility of this tool much greater. As discussed in the original SAFE papers, IDS provides the most value when it is tuned to the environment in which it is deployed. Depending on the voice control protocols used in your environment the tuning characteristics will be different. However in general, the number of traffic flows in the voice segment verses the data segment is much more easily classified. In the *controlling the voice-to-data segment interaction axiom*, a total of 8 flows were identified. The benefit of such a small set of traffic flows is twofold. First, any traffic other than those flows should trigger NIDS to alarm with high severity. This provides the defense in depth approach to attack mitigation. Second, given this small number of flows, filtering out false positives is relatively straightforward. In comparison this is far different than in the data segment where multiple flow exists and false positives are commonplace. Since attack signature detection in the voice segment is most likely not a false positive, you should consider enabling NIDS reactive features.

NIDS provides two features in additional to the monitoring described earlier. Once an attack signature is detected on a segment, shunning can be used to dynamically change the Layer 3 filtering configuration of a network device to drop all additional traffic from the source on that segment. Resets can be used to tear down a Transmission Control Protocol (TCP) session that triggers an attack signature. These features could be used however the reader is strongly encouraged to familiarize themselves with the guidelines provided in the original SAFE paper regarding shunning. For example, NIDS resets will provide attack mitigation for attacks against the call-processing manager web and IP phone services. NIDS shunning could be used to block UDP flood attacks sourced from the data segment against the voice segment however care should be taken to not block legitimate usage.

Many precautions should be taken directly on the voice-mail and call-processing manager systems as well. These include: turning off all unneeded services, patching the OS and services with the latest security patches, hardening the OS configuration, disabling any features on the voice servers that are not in use, and finally, not running any unnecessary applications on the server (for example, an e-mail client). Doing all these tasks reduces the number of vectors into the system an attack might use. Installing a host-based IDS (HIDS) is also recommended. Given the high target value of a voice server and the lag time involved in validating an application/OS security patch for production use, HIDS will provide significant and immediate attack mitigation. Some call-processing managers do not support HIDS. Installation of HIDS on the mail server in the data segment should also occur if this system is being used as the voice-mail store in addition to email content filtering or virus scanning. These recommendations are consistent with the SAFE security papers which recommend HIDS on all critical servers.

Voice servers may run multiple services that can be distributed across multiple devices in order to increase scalability and manageability. You should also use this feature to increase the level of security. For instance, call-processing managers typically support call control, web configuration, IP phone browsing services, conference calling, and device configuration services. Most configuration services do not support strong authentication. By segmenting these services the number of entry points into a system is reduced. Also make sure that the services use user or service accounts with only the privileges absolutely necessary to run normally. A compromised service shouldn’t provide root or administrative access.

Voice servers also support a variety of methods for management. These include protocols such as HTTP, Secure Sockets Layer (SSL), and Simple Network Management Protocol (SNMP). Follow the guidelines provided in the original SAFE paper regarding management operations.

Branch versus Headend Considerations

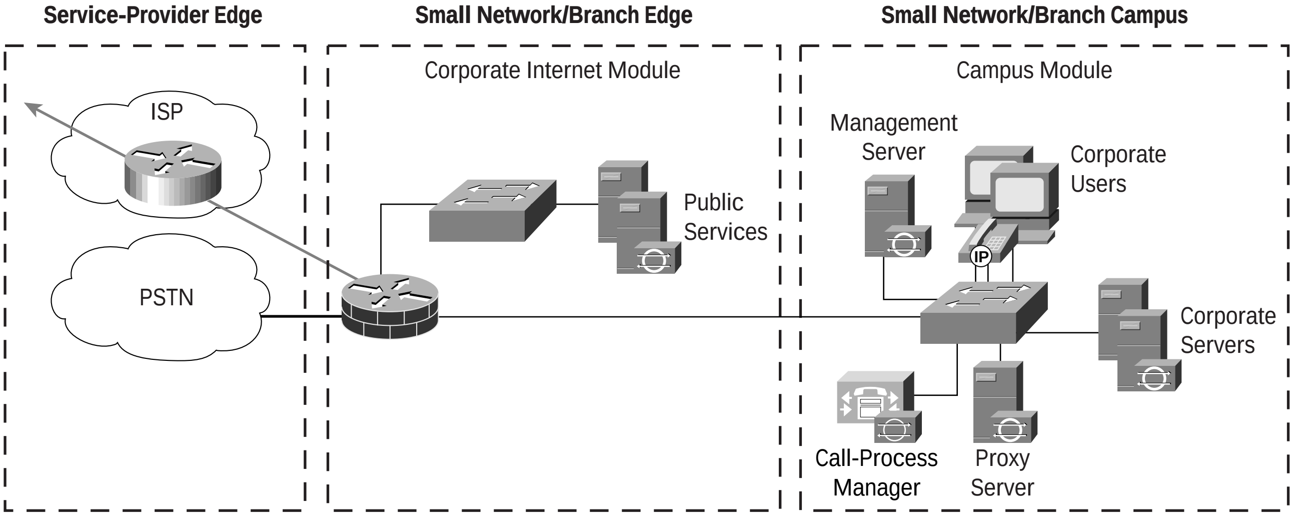
The small and medium designs that follow can be used in two possible configurations. In the first, the design is acting as a branch of a larger organization, built in the configuration described in SAFE Enterprise. In the second configuration, the design is the "headend" of an organization's network. This headend may have connections to other offices of the same organization. For example, a large law office may use the medium network design for its headend, and several small network designs for its other locations.

Still another example is a large automotive company that might use the SAFE enterprise design for its corporate headquarters, and many of the designs discussed in this paper for its remote locations. Where appropriate, the specific changes that may be required to a design are discussed in each section.

Small IP Telephony Design

The small IP telephony design utilizes the small network design from the SAFE security papers. The corporate Internet module has been modified to support voice services inluding Public Switched Telephone Network (PSTN) access for WAN backup and local calls, and VLANs for data/voice segmentation. The campus has been modified to support IP phones, PC-based IP Phones, proxy services, and VLANs. Most of the discussion in this design is based on this design operating as the headend for a corporation. Specific design changes when used as a branch are also included. The entire small business design is shown in Figure 2 for reference:

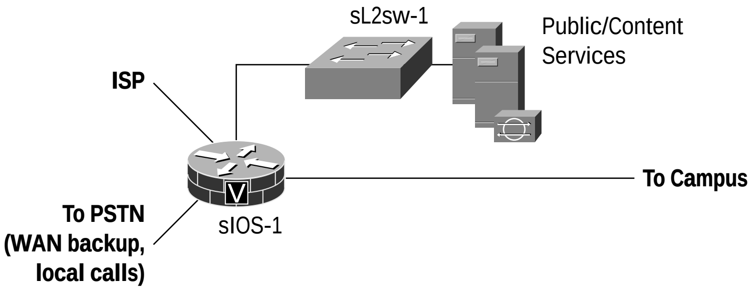
Figure 2
Small Network Detailed Model



Corporate Internet Module

The corporate Internet module provides internal users with connectivity to Internet services, Internet users access to information on public servers, and segmentation between the data and voice segments (located in the campus module). Figure 3 gives a diagram of the small network corporate Internet module.

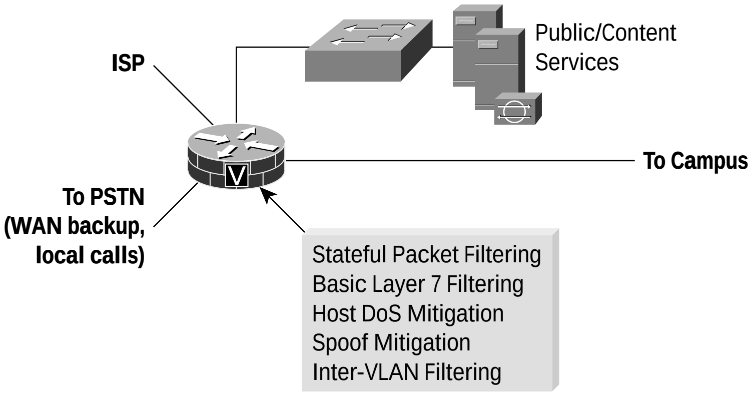
Figure 3
Small Network Corporate Internet Module: Detailed



Key IP Telephony Devices

- *Voice-enabled firewall router*—Provides network-level protection of resources, stateful filtering of traffic, and voice services (refer to Figure 4)

Figure 4
Small Network Corporate Internet Module: IP Telephony Detail



Voice Threats Mitigated

- *Unauthorized access*—This type of access is mitigated through filtering at the firewall.
- *Toll fraud*—Access control limits only known telephony devices from communicating with one another.
- *Denial of service*—TCP setup controls limit exposure to the call-processing manager.
- *IP spoofing*—RFC 2827 and 1918 filters are placed at the Internet service provider (ISP) edge and local firewall router.

Design Guidelines

This module represents the ultimate in scaled-down network design where all the features are compressed into a single box. These features include routing, NAT, IDS, VLAN, voice services, VPN, and stateful firewall. Two principal alternatives were considered in the original SAFE security papers. The first was to use a router. This setup yielded the greatest flexibility for the small network because the router supports all the advanced services that may be necessary in today's networks. As an alternative, a dedicated firewall was also considered. However, the dedicated firewall places numerous general and IP telephony-specific restrictions on deployment:

- First, firewalls are generally Ethernet only, requiring some conversion to access PSTN and the WAN. This access would then most likely occur through the use of an additional router, a setup that would nullify the choice of using a single dedicated firewall in the first place.
- Second, firewalls in this small scale of a design generally do not support enough interfaces or VLANs to provide segmentation between the Internet edge, public service, data, and voice segments.
- Third, for the branch mode of operation, firewalls do not support the same backup voice services for local call processing that routers do in case of headend failure. In a small network design where redundant links are not feasible, local backup call processing provides significant value.

Two VLANs exist. The call-processing manager, proxy server, and IP phones reside in the voice segment. All other devices including management, user, and the voice-mail/mail system reside in the data segment.

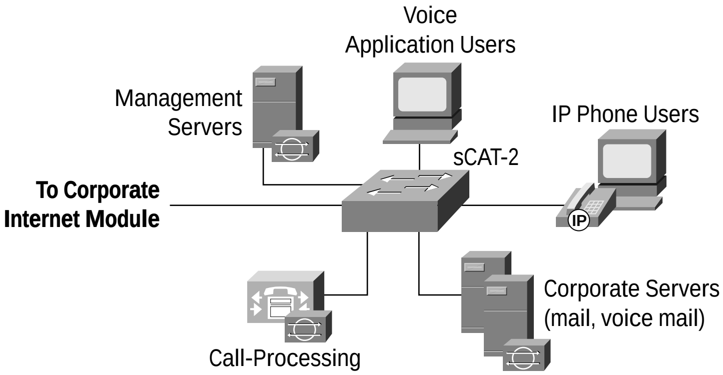
Access Control and Packet Inspection

The router controls access between the data and voice segments via access control and stateful inspection. Because the call-processing center and IP phones reside in the same voice segment, access control is not possible between the two. The router controls access to all other flows listed in the *controlling the voice-to-data segment interaction is key* axiom. Any other flows are denied and logged. Integrated IDS will alarm on any attack signatures detected in any of the above connections with the caveats outlined in the axioms section. In addition it should be noted that integrated IDS in routers and firewalls does not provide the full signature or feature set that a standalone NIDS appliance provides.

Campus Module

The campus module contains end-user workstations, corporate intranet servers, management servers, IP phones, and the associated Layer 2 infrastructure required to support the devices. Within the small network design, this Layer 2 functionality has been combined into a single switch.

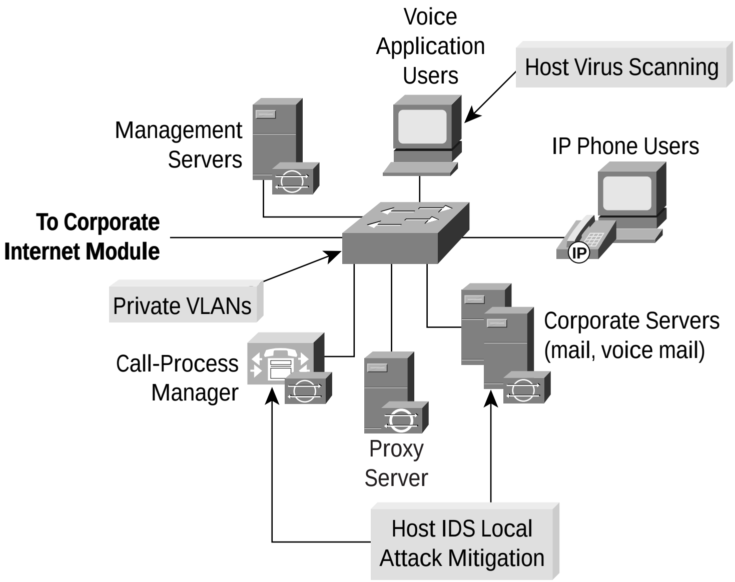
Figure 5
Small Network Campus Module: Detailed



Key IP Telephony Devices

- *Layer 2 switch (with VLAN support)*—Provides Layer 2 services to data and voice devices
- *Corporate servers*—Provide e-mail and voice-mail services to internal users, as well as delivering file, print, and Domain Name System (DNS) services to workstations
- *User workstations*—Provide data services and voice services via PC-based IP Phones to authorized users on the network
- *IP phones*—Provide voice services to users on the network
- *Call-processing manager*—Provides voice services to IP telephony devices in the network
- Proxy Server—Provides data services to IP phones

Figure 6
Small Network Campus Module: IP Telephony Detail



Voice Threats Mitigated

- *Packet sniffers/call interception*—A switched infrastructure limits the effectiveness of sniffing.
- *Virus and Trojan-horse applications*—Host-based virus scanning prevents most viruses and many Trojan horses.
- *Unauthorized access*—This type of access is mitigated through the use of HIDS and application access control.
- *Application layer attacks*—Operating systems, devices, and applications are kept up-to-date with the latest security fixes, and most servers are additionally protected by HIDS.
- *Caller identity spoofing*—Arpwatch notifies the administrator of the unknown device.
- *Toll fraud*—The call-processing manager will not allow unknown phones to be configured.
- *Denial of service*—Separation of the voice and data segments significantly reduces the likelihood of an attack.
- *Repudiation*—Users are authenticated before accessing the telephony device, thus reducing the likelihood of a later denial that a call ever occurred.
- *Trust exploitation*—Restrictive trust model and private VLANs to limit trust-based attacks

Design Guidelines

The primary functions of the campus switch are to switch data, management, and voice traffic and to provide connectivity for the corporate, voice, and management servers and users. These functions are carried out via VLAN support and reliance on HIDS and virus scanning on key systems. A unified voice-mail/email server was placed in the data segment given the small scale and the limited number of voice segments. This placement further restricted the number of hosts accessing the sole voice segment.

Access Control and Packet Inspection

Within the Layer 2 switch, VLANs are enabled in order to mitigate attacks sourced from the data segment against the voice segment. Because there are no Layer 3 services within the campus module, it is important to note that this design places an increased emphasis on application and host security because of the open nature of the internal network. Therefore, HIDS was also installed on key systems within the campus, including the corporate servers, call-processing manager, and management systems.

Because this network is so small and only a single voice and single data segment exist, it is actually more feasible than in a larger design to deploy a firewall between the two segments. Thus, deployment of PC-based IP Phones in the data segment is more feasible as the stateful firewall functionality of the router can broker the data-voice interaction. However, the remaining issues covered in the *PC-based IP phones require open access* axiom still hold. Virus scanning was installed on user systems. This provided virus/worm attack mitigation for the PC-based IP Phone hosts against attacks on the data segment. If the hosts were infected, the virus/worm could potentially spread and attack the voice segment. HIDS detects any anomalies on the mail, voice-mail, or call-processing devices. Access control is not carried out in this module. The proxy server is located on the same VLAN as the call-processing manager however private VLANs are enabled to mitigate local trust-exploitation attacks.

Performance and Scalability

For the standalone network design, the scalability limit is the number of IP telephony devices supported by the local call-processing manager and voice-mail system. Performance in this design is not an issue because all necessary services are available locally on a Fast Ethernet switched network.

Secure Management

Layer 3 and Layer 4 filtering was put in place to limit the administration of the voice servers by known management systems. Application-level security was used to provide confidentiality and user authentication for the configuration and monitoring management traffic. IP phones download the latest configurations and OS versions from the call-processing manager at regular intervals.

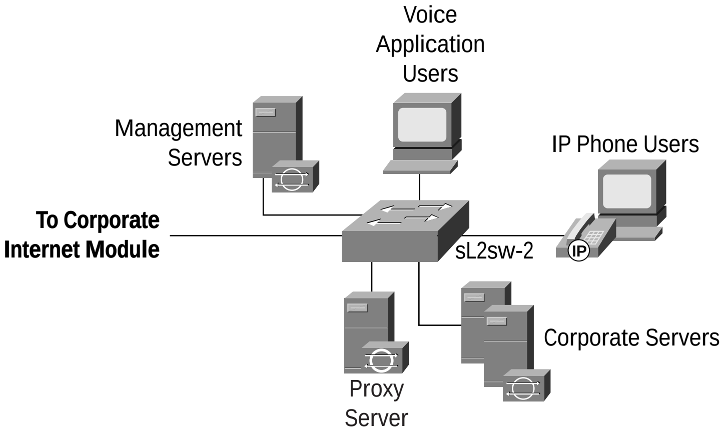
Alternatives

The first logical modification to the design would be to deploy two seperate voice segments: one for IP phones and the other for the call-processing manager. This configuration would provide additional connection management between user and telephony service systems than that provided by the single segment today. The design would then be very similar to that of the medium campus IP telephony design. You might also consider placing the voice-mail/e-mail server in the voice segment. However, this is not recommended. Most likely the mail server is running multiple services. For instance, in this design the mail server also operates as the domain controller and DNS server. The associated risk is great enough to keep it separate than on the same segment as the IP phones and call-processing manager.

Branch versus Standalone Considerations

Figure 7

Small Branch Network Campus Module: Detailed

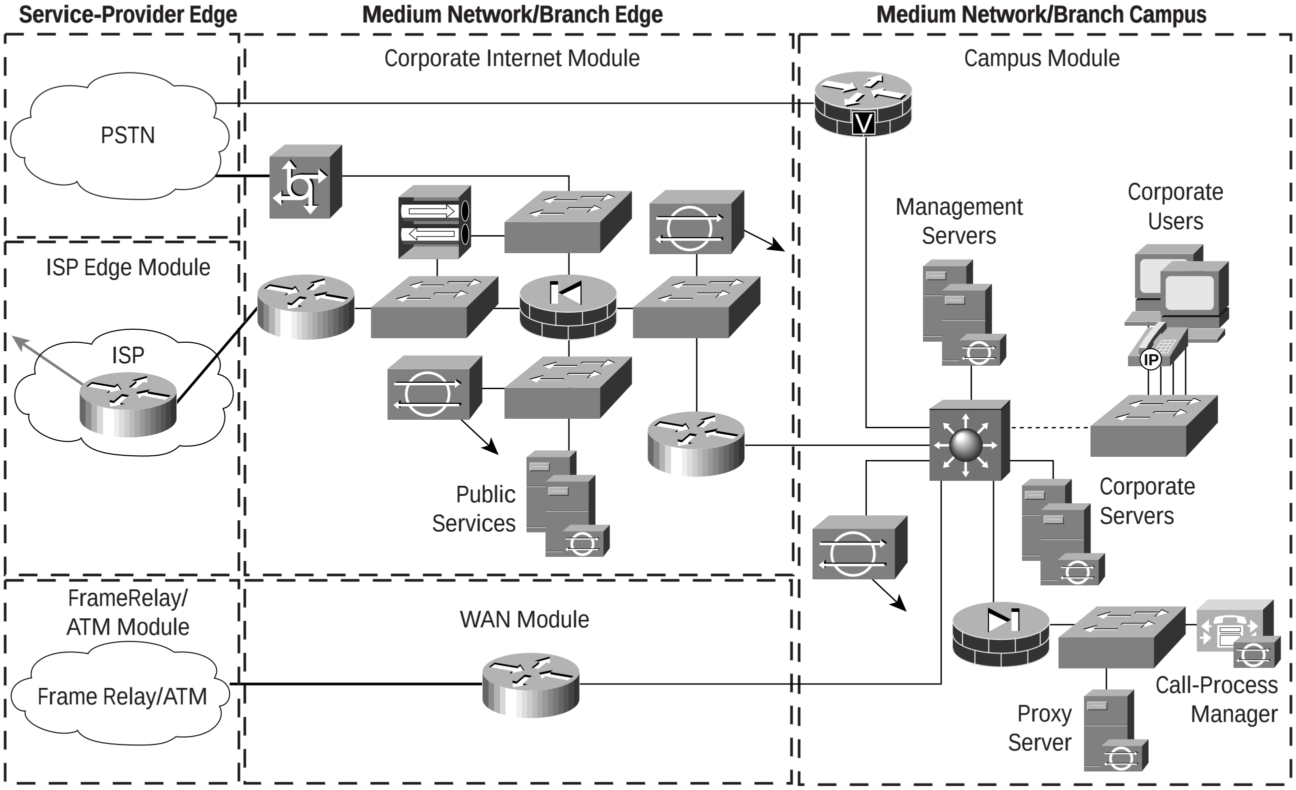


The primary consideration between the two designs is the location of the voice services. Because the voice services are located remotely in the branch design, configuration of the firewall router will be more complex to allow the connections as outlined in the *controlling the voice-to-data segment interaction is key* axiom. This setup increases the likelihood of configuration errors. The branch design requires a different software image supporting call processing on the router in case of headend failure. This requirement constitutes the only difference in the corporate Internet module for both designs. The number of telephony devices supported will be limited first by the headend call-processing manager and the voice-mail system. The second limiting factor is the number of devices supported by the voice-enabled router in the corporate Internet module in case of headend failure. Performance may also be limited by the slower response time of the call-processing manager and voice-mail systems located at the headend.

Medium IP Telephony Design

The medium IP telephony design utilizes the medium network design from the SAFE security papers. The corporate Internet module has not been modified. The campus module has been modified to support IP phones, PC-based IP Phones, voice services, proxy services, PSTN for WAN backup and local calls, and VLANs for data/voice segmentation. Most of the discussion in this design is based on this design operating as the headend for a corporation. Specific design changes when used as a branch are also included. The entire medium business design is shown here for reference:

Figure 8
Medium Network Detailed Model

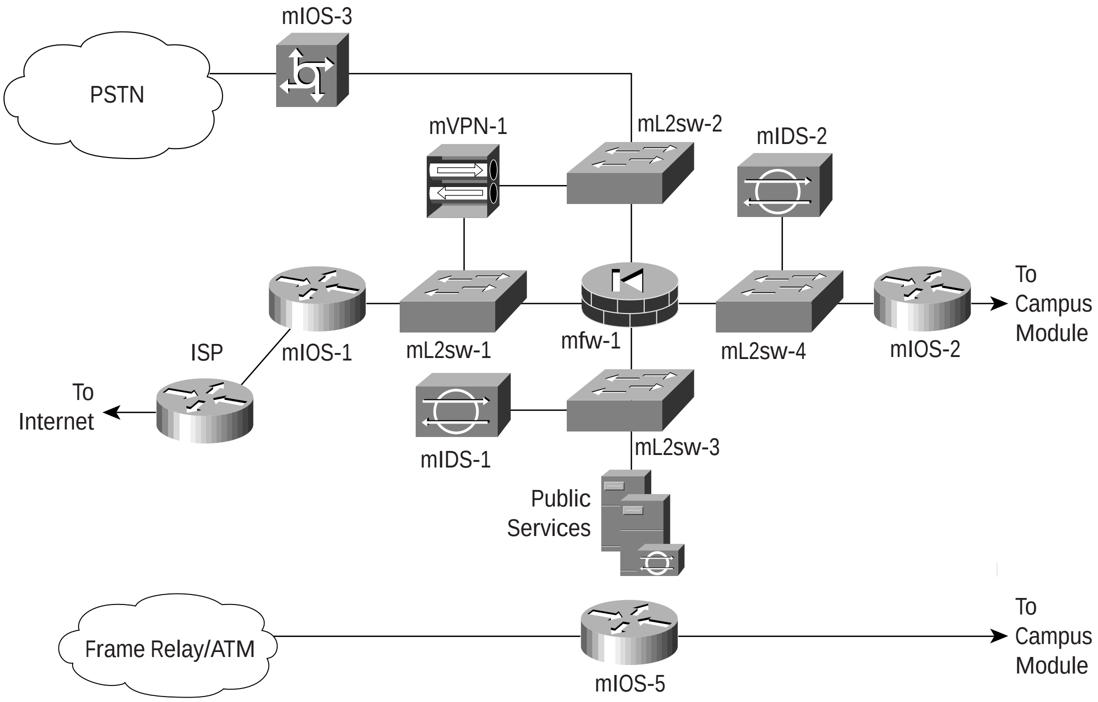


Medium Edge Design

The corporate Internet module provides internal users with connectivity to Internet services and Internet users access to information on the public servers (HTTP, FTP, Simple Mail Transfer Protocol (SMTP), and DNS). The WAN module provides connections to remote locations over a private network. No required changes were made to the corporate Internet module to support IP telephony; however, it is provided in Figure 9 for reference.

Figure 9

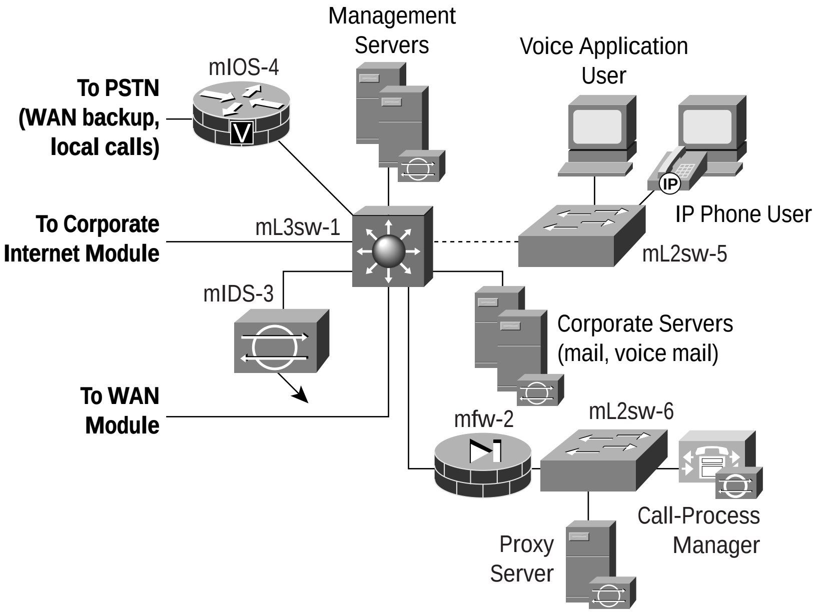
Medium Network Corporate Internet Module: Detailed



Campus Module

The original campus module contained end-user workstations, corporate servers, management servers, and the associated Layer 2 and Layer 3 infrastructure required to support the devices. Its primary purpose is to switch production and management traffic and to provide connectivity for the corporate and management servers and users. To support IP telephony, Cisco has added IP phones, voice servers, a proxy server, additional voice VLANs, and a call-processing manager with a stateful firewall to protect it.

Figure 10
Medium Campus Module: Detailed

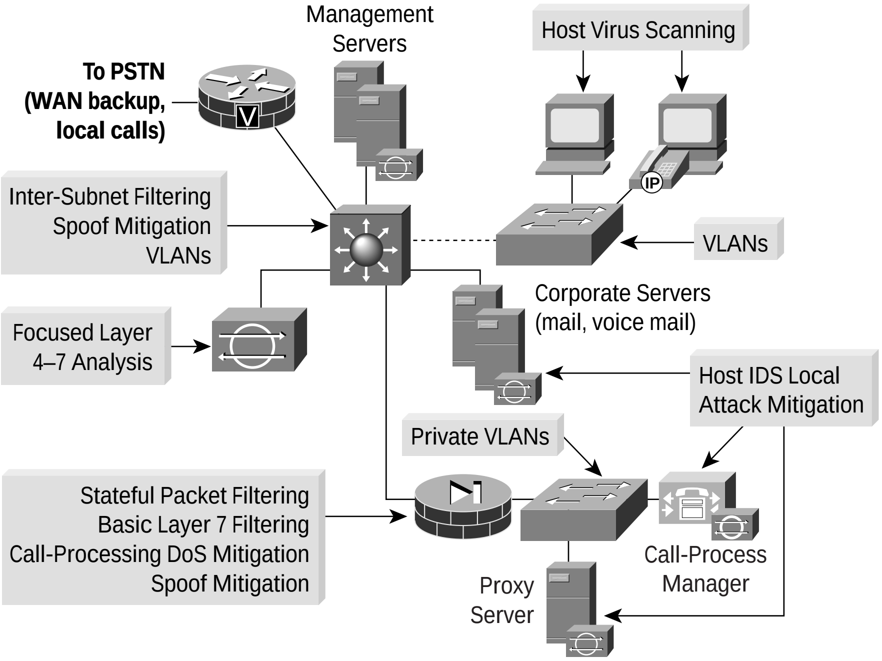


Key IP Telephony Devices

- *Layer 3 switch*—Route and switch data, voice, and management traffic within the campus module provide distribution layer services to the building switches, and support advanced services such as traffic filtering.
- *Layer 2 switch (with VLAN support)*—The Layer 2 switch provides Layer 2 services to data and voice devices.
- *Corporate servers*—Corporate servers provide e-mail and voice-mail services to internal users, as well as delivering file, print, and DNS services to workstations.
- *User workstations*—User workstations provide data services and voice services via PC-based IP Phones to authorized users on the network.
- *NIDS appliance*—A NIDS appliance provides Layer 4-to-Layer 7 monitoring of key segments in the module.
- *IP phones*—IP phones provide voice services to users on the network.
- *Call-processing manager*—This feature provides voice services to IP telephony devices in the network.
- *Stateful firewall*—The stateful firewall provides network level protection for the call-processing manager, including stateful filtering of traffic, DoS mitigation, and spoof mitigation.
- *Proxy Server*—Provides data services to IP phones

Figure 11

Medium Campus Module: IP Telephony Detail


Management Servers
Host Virus Scanning
To PSTN (WAN backup, local calls)
V
IP
Inter-Subnet Filtering
Spoof Mitigation
VLANs
VLANs
Corporate Servers (mail, voice mail)
Focused Layer 4–7 Analysis
Host IDS Local Attack Mitigation
Private VLANs
Stateful Packet Filtering
Basic Layer 7 Filtering
Call-Processing DoS Mitigation
Spoof Mitigation
Call-Process Manager
Proxy Server

Voice Threats Mitigated

- *Packet sniffers/call interception*—A switched infrastructure limits the effectiveness of sniffing.
- *Virus and Trojan-horse applications*—Host-based virus scanning prevents most viruses and many Trojan horses.
- *Unauthorized access*—This type of access is mitigated through the use of HIDS and application access control.
- *Application layer attacks*—Operating systems, devices, and applications are kept up-to-date with the latest security fixes, and most servers are additionally protected by HIDS.
- *Caller identity spoofing*—Arpwatch notifies the administrator of the unknown device
- *Toll fraud*—The call-processing manager will not allow unknown phones to be configured. Access control limits only known telephony networks from communicating with one another.
- *Denial of service*—Separation of the voice and data segments significantly reduces the likelihood of an attack. The stateful firewall TCP setup controls limit exposure to the call-processing manager and proxy server.
- *Repudiation*— Call-processing manager call setup logs provide some level of nonrepudiation.
- *IP spoofing*—RFC 2827 and 1918 filters are placed at the ISP edge and local firewall.

Design Guidelines

The primary function of the campus module is to switch data, voice, and management traffic and at the same time enforce the data network and voice segmentation. These functions are carried out by VLANs and filtering on both the Layer 3 switch and stateful firewall. Virus scanning protects PC-based IP Phone hosts on the data segment. HIDS protects key voice services.

Access Control and Packet Inspection

The Layer 3 switch controls access between the data and voice segments via access control and stateless filtering. The Layer 3 switch filters all flows listed in the *controlling the voice-to-data segment interaction is key* axiom. These connections are brokered by the stateful firewall. Any other flows between the voice and data segments are denied and logged by filtering on either the Layer 3 switch or the stateful firewall. Network IDS alarms on any attack signatures detected in any of these connections with the caveats outlined in the axioms section. HIDS detects any anomalies on the mail, voice-mail, or call-processing devices. Virus scanning was installed on user systems to provide attack mitigation for the PC-based IP Phone against attacks on the data segment that could then traverse into the voice segment. The proxy server is located on the same VLAN as the call-processing manager however private VLANs are enabled to mitigate local trust-exploitation attacks.

Performance and Scalability

For the standalone network, the limit of this design is the number of IP telephony devices supported by the local call-processing manager and voice-mail system. Performance in this design is not an issue because all necessary services are available locally on a Fast Ethernet switched network.

Secure Management

Layer 3 and Layer 4 filtering was put in place to limit the administration of the voice servers by known management systems. Application-level security was used to provide confidentiality and user authentication for the configuration and monitoring management traffic. IP phones download the latest configurations and OS versions from the call-processing manager at regular intervals.

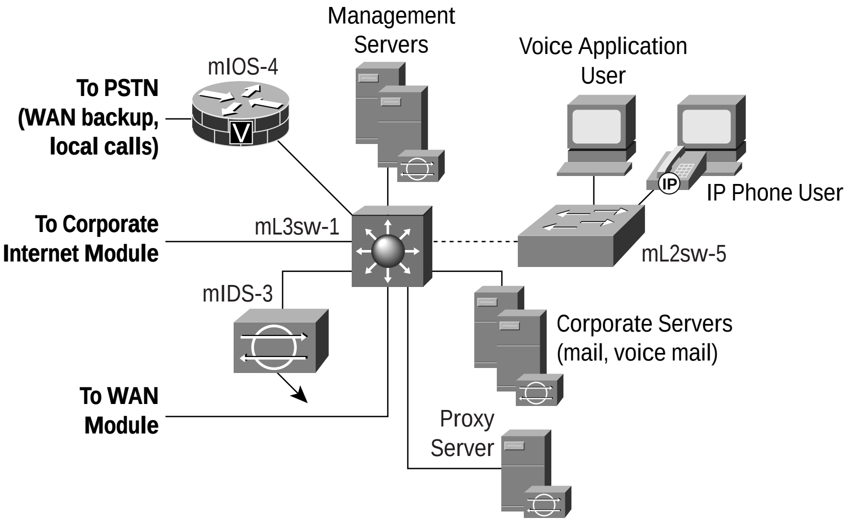
Alternatives

One alternative would be the addition of high availability for IP telephony. An administrator might consider adding a resilient firewall pair and an additional call-processing manager to accomplish this. This design would then be similar to the enterprise IP telephony design. Another option would be to place the voice-mail system off of an additional DMZ segment on the stateful firewall. This setup would provide for stateful inspection and filtering between the telephony devices and the voice-mail system instead of the current stateless filtering. This option would also provide DoS mitigation for the voice-mail system and stateful inspection between it and the mail server in the data segment. The only real drawback to this option is the increasing complexity of the configuration.

Branch versus Standalone Considerations

Figure 12

Medium Branch Network Campus Module: Detailed



The primary consideration when using this design in a branch configuration is the location of the call-processing manager. Because the call-processing manager is located remotely in the branch design, configuration of the Layer 3 switch will be more complex to allow the connections as outlined in the *controlling the voice-to-data segment interaction is key* axiom. This scenario increases the likelihood of configuration errors. In the branch design, performance may be limited by the slower response time of the call-processing manager located at the headend. Calls are transported to the headend via the WAN module.

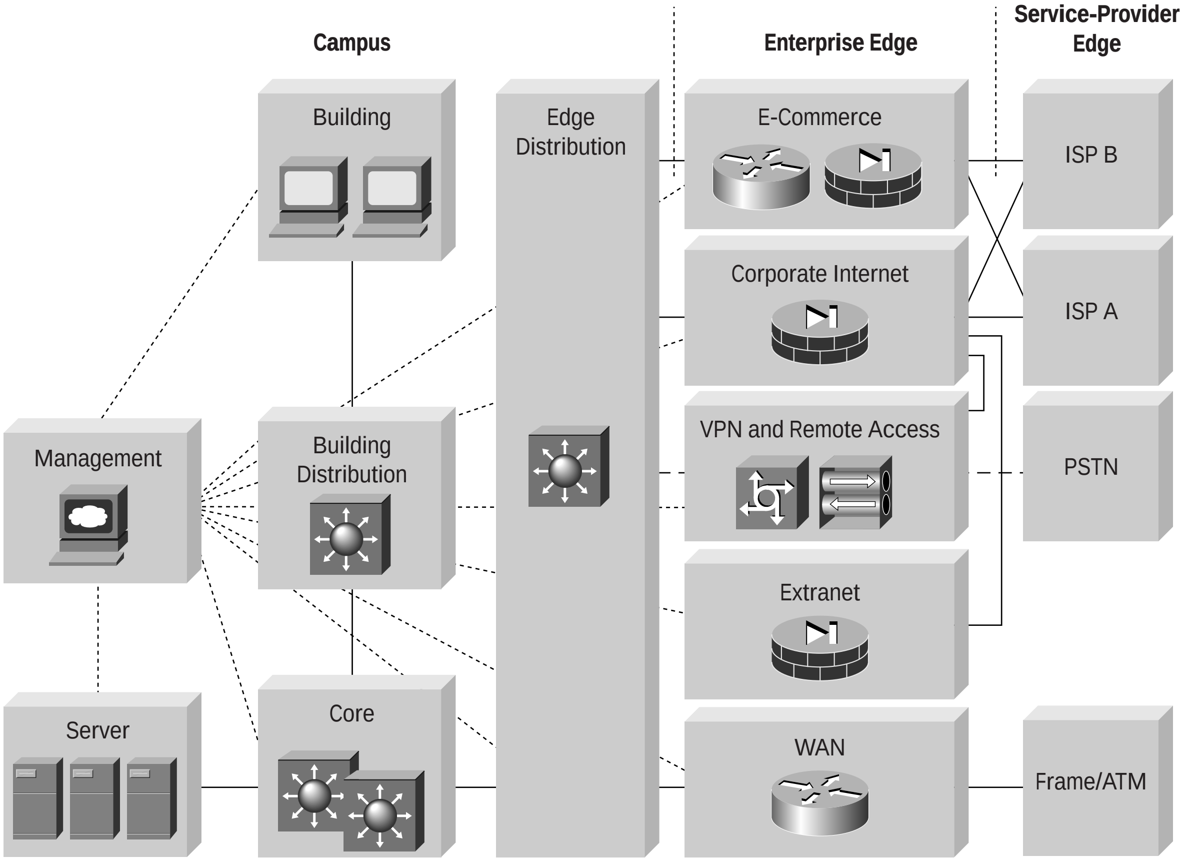
Large IP Telephony Design

The large IP telephony design utilizes the large network design from the SAFE enterprise paper. IP telephony was available in the initial release of the paper but not discussed in depth. Some changes have been made to the design, including:

- PC-based IP Phones were added to the data segments of the R&D and marketing user groups.
- An additional voice segment was added for the voice-mail system.
- PSTN for local calls was added to the edge distribution module.
- The call-processing segment in the server module was made highly available and front ended with a pair of stateful firewalls.
- HIDS was installed on all voice-related services.
- NIDS was tuned to the correct flows in the voice and related segments.

The entire enterprise design is shown in Figure 13 for reference:

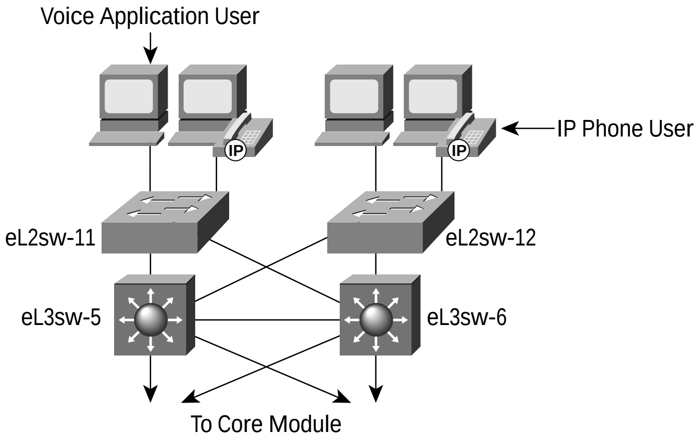
Figure 13
Large Network Detailed Model



Building Module

The building module contains end-user workstations, IP phones, and their associated Layer 2 access points. Its primary goal is to provide services to end-users. The topology of the building module remains unchanged from the original SAFE paper, but some of the mitigation factors have changed.

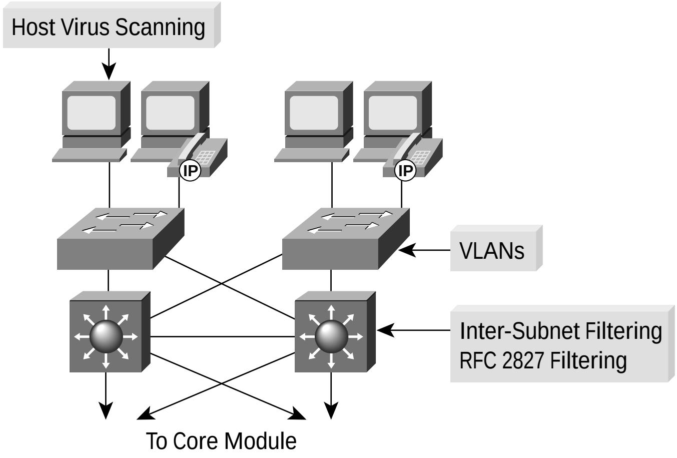
Figure 14
Enterprise Building Module: Detailed



Key IP Telephony Devices

- *Layer 2 switch (with VLAN support)*—This switch provides Layer 2 services to data and voice devices.
- *User workstations*—User workstations provide data services and voice services via PC-based IP Phones to authorized users on the network.
- *IP phones*—IP phones provide voice services to users on the network.

Figure 15
Enterprise Building Module: IP Telephony Detail



Voice Threats Mitigated

- *Packet sniffers/call interception*—A switched infrastructure limits the effectiveness of sniffing.
- *Virus and Trojan-horse applications*—Host-based virus scanning prevents most viruses and many Trojan horses.
- *Unauthorized access*—This type of access is mitigated through the use of HIDS and application access control.
- *Caller identity spoofing*— Arpwatch notifies the administrator of the unknown device.
- *Toll fraud*—Access control limits only known telephony networks from communicating with one another.
- *Repudiation*—Call-processing manager call setup logs provide some level of nonrepudiation.
- *IP spoofing*—RFC 2827 and 1918 filters are placed on the Layer 3 switches.

Design Guidelines

The primary function of the building module is to switch data and voice traffic and at the same time enforce the data and voice segmentation. These functions are carried out by stateless Layer 3 filtering and VLANs. Virus scanning protects user systems on the data segment.

SAFE wireless LAN security in depth discusses the fact that user-group differentiation is not possible with today's wireless technology unless IPSec is used. A recommendation was made to disallow users on a wireless segment from accessing a controlled group segment with the understanding that the risks outweighed the benefits. This best practice has been followed throughout the updated enterprise design.

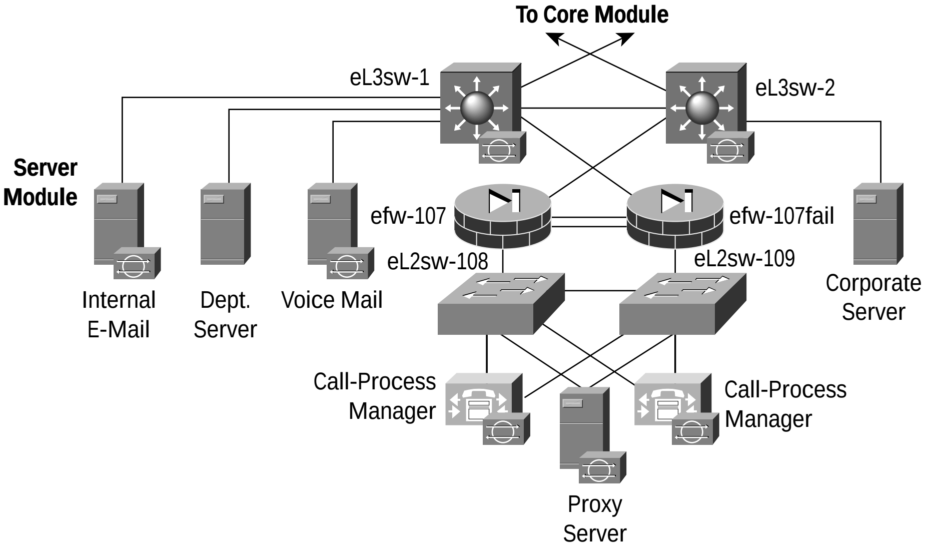
Access Control and Packet Inspection

Within the switches, VLANs are enabled in order to mitigate attacks sourced from the data segment against the voice segment. Stateless Layer 3 filtering controls the flows outlined in the *controlling the voice-to-data segment interaction is key* axiom. Any other flows are denied and logged. Virus scanning was originally installed to mitigate local attacks on the user systems. Since they are now running the PC-based IP Phone and have access to the voice segment, attack mitigation on these hosts is key to guard against attacks on the data segment from traversing into the voice segment.

Enterprise Server Module

The primary goal of the server module is to provide application and voice services to end users and devices.

Figure 16
Enterprise Server Module: Detailed

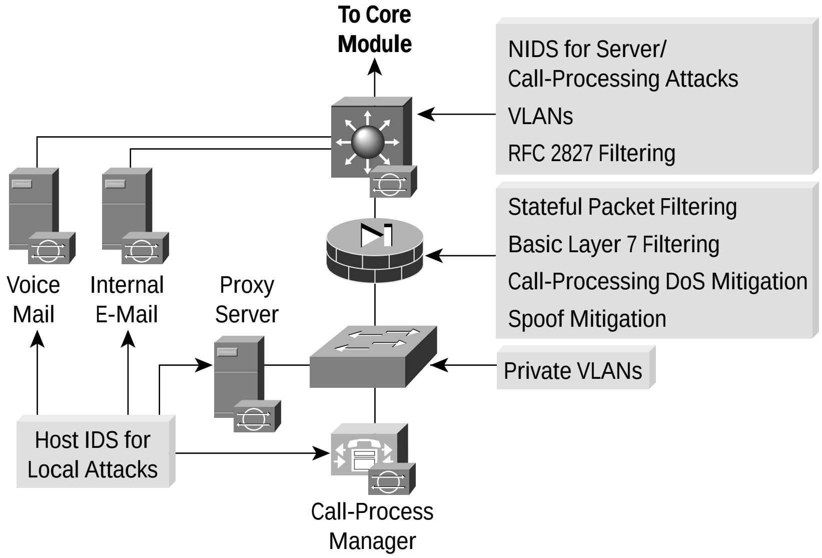


Key IP Telephony Devices

- *Layer 3 switch*—The Layer 3 switch routes and switches data, voice, and management traffic within the server module, and supports advanced services such as traffic filtering and NIDS.
- *Corporate servers*—Corporate servers provide e-mail and voice-mail services to internal users, as well as delivering file, print, and DNS services to workstations.
- *Call-processing manager*—The call-processing manager provides voice services to IP telephony devices in the network.
- *Stateful firewall*—The stateful firewall provides network level protection for call-processing manager, including stateful filtering of traffic, DoS mitigation, and spoof mitigation.
- *Proxy Server*—Provides data services to IP phones

Figure 17

Enterprise Server Module: IP Telephony Detail



Voice Threats Mitigated

- *Packet sniffers/call interception*—A switched infrastructure limits the effectiveness of sniffing.
- *Unauthorized access*—This type of access is mitigated through the use of HIDS and application access control.
- *Caller identity spoofing*— Arpwatch notifies the administrator of the unknown device.
- *Toll fraud*—The call-processing manager will not allow unknown phones to be configured. Access control limits only known telephony networks from communicating with one another.
- *Repudiation*—Call-processing manager call setup logs provide some level of nonrepudiation.
- *IP spoofing*—IP spoofing provides RFC 2827 and 1918 filtering on Layer 3 switches and stateful firewall.
- *Application layer attacks*—Operating systems, devices, and applications are kept up-to-date with the latest security fixes, and most servers are additionally protected by HIDS.
- *Denial of service*—Separation of the voice and data segments significantly reduces the likelihood of an attack. The stateful firewall TCP setup controls limit exposure to the call-processing manager and proxy server.
- *Trust exploitation*—Restrictive trust model and private VLANs to limit trust-based attacks

Design Guidelines

The server module contains all the voice services necessary for IP telephony. The call-processing manager, proxy server, voice-mail, and mail systems reside in separate segments not only to model the scale of a large enterprise but also to provide layered security. All services have HIDS agents installed. All traffic flows in the server module are inspected by onboard IDSs within the Layer 3 switches. The call-processing segment is highly available and is protected by a stateful firewall pair.

Access Control and Packet Inspection

Segmenting the services offers tremendous value in both scalability and security. It is easier to implement the required flows as outlined in the *controlling the voice-to-data segment interaction is key* axiom, reducing the likelihood of configuration errors. Any other flows are denied and logged. If NIDS detects a signature, the system will alarm with the caveats outlined in the axioms section. HIDS detects anomalies on the mail, voice-mail, or call-processing devices. The proxy server is located on the same VLAN as the call-processing manager however private VLANs are enable to mitigate local trust-exploitation attacks.

Performance and Scalability

The scalability limit is the number of IP telephony devices supported by the call-processing manager and voice-mail system. Performance in this design is not an issue because all necessary services are available locally on a Fast Ethernet switched network, with the exception of some remote sites that use these local services over the WAN.

High Availability

This module continues to provide Layer 2 and Layer 3 resiliency as it did in the original SAFE paper. With the addition of voice services, high availability was maintained. Two stateful firewalls connect the secured call processing manager segment to the dual Layer 3 switches in the server module. The internal segment is Layer 2 resilient not only between the firewalls' internal interfaces and the dual Layer 2 switches, but also on the dual-interfaced call processing managers as well. In this configuration each call processing manager operates with two network interface cards, both in the same network, with one connected to each switch.

Secure Management

The enterprise SAFE security design supported out-of-band (OOB) secure management as one potential management option. Meaning all network devices and all key servers were dual-homed to provide a dedicated and secure interface for management. In comparison, devices can be managed in-band over existing segments however this mixes the production and management traffic and thus makes it more difficult to secure the device. For more information on OOB management please refer to the SAFE enterprise paper. As it relates to IP telephony, all voice servers should support more than one interface to support this best practice. The voice services are critical components of the network and restricting management access to them is key in safeguarding them from attack. Layer 3 and Layer 4 filtering was put in place to limit the administration of the voice servers by known management systems. Application-level security was used to provide confidentiality and user authentication for the management traffic.

Alternative

One option would be to place the voice-mail system off of an additional DMZ segment on the stateful firewalls. This setup provides for stateful inspection and filtering between the telephony devices and the voice-mail system instead of the current stateless filtering. This option also provides DoS mitigation for the voice-mail system and stateful inspection between it and the mail server in the data segment. The only real drawback to this option is the increased complexity of the configuration.

Appendix A: Validation Lab

A reference SAFE IP telephony implementation exists to validate the functionality described in this document. This appendix details the configurations of the specific devices as they relate to IP telephony functionality within each module. It details the configurations of the specific devices within each module, as well as the overall guidelines for general device configuration. The following are configuration snapshots from the live devices in the lab. The author does not recommend applying these configurations directly to a production network.

Protocols and ports used in the Cisco proof-of-concept SAFE lab.

Application	Protocol	Port(s)
DHCP	UDP	67/68
HTTP	TCP	80
RTP	UDP	16384-32767
TAPI/JTAPI	TCP	2748
Cisco Softphone Directry Lookup	TCP	389/8404
Cisco Skinny	TCP	2000
HIDS Management	TCP	5000

IP Telephony Devices Used in Validation

- Cisco CallManager 3.1(2) was used for the “call-processing manager.”
- Cisco 7960 IP phones running Cisco Skinny Station Protocol for call control were used for the “IP phones.”
- Cisco Unity™ 3.1(2c)SpB was used for the “voice-mail server.”
- Cisco SoftPhone 1.2(2) was used for the “PC-based IP Phone.”
- Microsoft Exchange 2000 SP1 was used for the “mail server.”

Security Devices Used in Validation

- Cisco PIX® Firewall 6.1.1(105) was used for the “stateful firewall.”

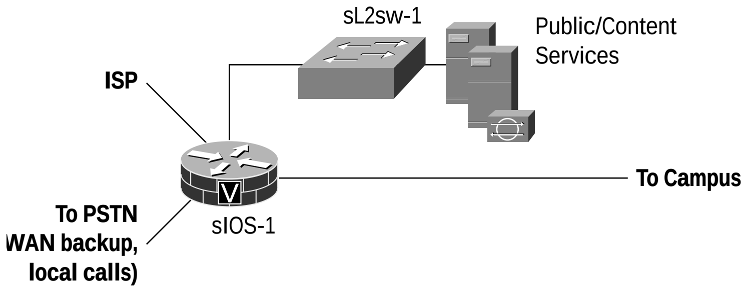
Configuration Notes

All the following configurations include support for the Cisco SoftPhone. Due to the date/voice segment interaction required, supporting SoftPhone complicates the configurations considerably. The Dynamic Host Configuration Protocol (DHCP) server is shown on a Cisco router in order to demonstrate how to associate a known Media Access Control (MAC) with an IP address assignment. You may choose to use a different DHCP server and create a new scope instead; in this case, add the ip helper command to the associated interface.

Small IP Telephony Design

Small Standalone Corporate Internet Module

Figure A-1
Small-Site Standalone Corporate Internet Module



Voice-Enabled Firewall Router: sIOS-1

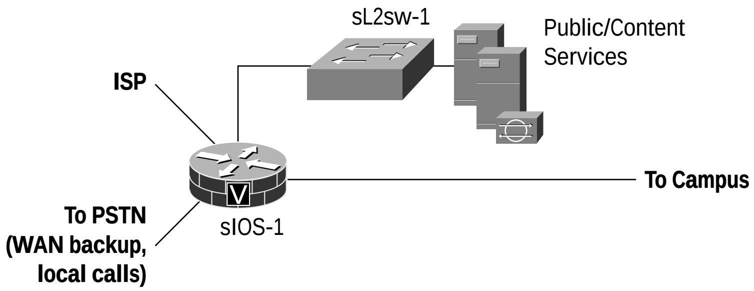
```
!addresses to exclude – default router, call manager, and broadcast
ip dhcp excluded-address 10.4.50.1
ip dhcp excluded-address 10.4.50.255
ip dhcp excluded-address 10.4.50.50
!
ip dhcp pool ip-phone-pool
   host 10.4.50.129 255.0.0.0
   client-identifier 0100.3094.c25d.df
   dns-server 10.4.1.201
   default-router 10.4.50.1
   domain-name safe-small.com

!ip address of CallManager
   option 150 ip 10.4.50.50

!Data VLAN
interface FastEthernet0/0
 ip address 10.4.1.1 255.255.255.0
 ip access-group 109 in
 no ip redirects
 ip nat inside
 ip inspect smbranch_fw in
 ip audit alarm1 in
 no cdp enable

! Voice VLAN
interface FastEthernet0/0.2
 encapsulation dot1Q 50
 ip address 10.4.50.1 255.255.255.0
 ip access-group 150 in
 ip inspect smbranch_fw in
 no cdp enable
```

```
!firewall/IDS config
ip inspect max-incomplete high 50000
ip inspect max-incomplete low 45000
ip inspect one-minute high 600000
ip inspect one-minute low 599000
ip inspect udp idle-time 20
ip inspect dns-timeout 3
ip inspect tcp idle-time 1800
ip inspect tcp finwait-time 3
ip inspect tcp synwait-time 15
ip inspect tcp max-incomplete host 40 block-time 0
ip inspect name smbranch_fw ftp
ip inspect name smbranch_fw http
ip inspect name smbranch_fw smtp
ip inspect name smbranch_fw tcp timeout 300
ip inspect name smbranch_fw fragment maximum 256 timeout 1
ip inspect name smbranch_fw tftp
ip inspect name smbranch_fw udp
ip audit attack action alarm drop reset
ip audit notify log
ip audit po max-events 100
ip audit name alarm1 info action alarm
ip audit name alarm1 attack action alarm drop

!Access-list for DATA segment
!some lines truncated, please see SAFE small, medium, and remote design for complete ACL
!permit Unity to talk to CallManager
access-list 109 permit tcp host 10.4.1.60 host 10.4.50.50 eq 2000

!permit Softphone (TAPI/JTAPI) to do call setup to CallManager
access-list 109 permit tcp 10.4.1.0 0.0.0.255 host 10.4.50.50 eq 2748

!permit Softphone to talk to IP Phones but not Call Manager
access-list 109 deny udp 10.4.1.0 0.0.0.255 host 10.4.50.50 range 16384 32767
access-list 109 permit udp 10.4.1.0 0.0.0.255 10.4.50.0 0.0.0.255

!permit users in the data segments to access the web server on CallManager
access-list 109 permit tcp 10.4.1.0 0.0.0.255 host 10.4.50.50 eq www

!deny all other data to voice vlan traffic
access-list 109 deny   ip 10.4.1.0 0.0.0.255 10.4.50.0 0.0.0.255

!RFC 2827 filtering
access-list 109 permit ip 10.4.0.0 0.0.255.255 any
access-list 109 deny   ip any any log

!Access-list for Voice VLAN
!permit DHCP to router
access-list 150 permit udp host 0.0.0.0 host 255.255.255.255

!permit CallManager to talk to Unity
access-list 150 permit tcp host 10.4.50.50 eq 2000 host 10.4.1.60

!permit HIDS agent on CallManager to talk to HIDS manager console
access-list 150 permit tcp host 10.4.50.50 host 10.4.1.253 eq 5000
```

```
!permit SoftPhone to do call setup to CallManager
access-list 150 permit tcp host 10.4.50.50 eq 2748 10.4.1.0 0.0.0.255

!permit users on the data segments to access the web server on the CallManager
access-list 150 permit tcp host 10.4.50.50 eq www 10.4.1.0 0.0.0.255

!permit calls between IP phones and SoftPhone, permit phones to leave messages on Unity
access-list 150 deny udp host 10.4.50.50 10.4.1.0 0.0.0.255
access-list 150 permit udp 10.4.50.0 0.0.0.255 10.4.1.0 0.0.0.255 range 16384 32767
access-list 150 deny   ip any any log
```

Configuration for Small Branch Corporate Internet Module

Figure A-2
Small-Site Branch Corporate Internet Module



Voice-Enabled Firewall Router: sIOS-1

```
!addresses to exclude – default router and broadcast
ip dhcp excluded-address 10.4.50.1
ip dhcp excluded-address 10.4.50.255
!
ip dhcp pool ip-phone-pool
   host 10.4.50.129 255.0.0.0
   client-identifier 0100.3094.c25d.df
   dns-server 10.4.1.201
   default-router 10.4.50.1
   domain-name safe-small.com

!ip address of CallManager
   option 150 ip 10.1.17.50

!Data VLAN
interface FastEthernet0/0
 ip address 10.4.1.1 255.255.255.0
 ip access-group 109 in
 no ip redirects
 ip nat inside
 ip inspect smbranch_fw in
 ip audit alarm1 in
 no cdp enable

! Voice VLAN
interface FastEthernet0/0.2
 encapsulation dot1Q 50
 ip address 10.4.50.1 255.255.255.0
 ip access-group 150 in
 ip inspect smbranch_fw in
 no cdp enable

!firewall/IDS config
ip inspect max-incomplete high 50000
ip inspect max-incomplete low 45000
ip inspect one-minute high 600000
ip inspect one-minute low 599000
ip inspect udp idle-time 20
ip inspect dns-timeout 3
ip inspect tcp idle-time 1800
ip inspect tcp finwait-time 3
ip inspect tcp synwait-time 15
ip inspect tcp max-incomplete host 40 block-time 0
ip inspect name smbranch_fw ftp
ip inspect name smbranch_fw http
ip inspect name smbranch_fw smtp
ip inspect name smbranch_fw tcp timeout 300
ip inspect name smbranch_fw fragment maximum 256 timeout 1
ip inspect name smbranch_fw tftp
ip inspect name smbranch_fw udp
ip audit attack action alarm drop reset
ip audit notify log
ip audit po max-events 100
ip audit name alarm1 info action alarm
ip audit name alarm1 attack action alarm drop

!Access-list for DATA segment
!some lines truncated, please see SAFE small, medium, and remote design for complete ACL
!permit Unity to talk to Primary CallManager
access-list 109 permit tcp host 10.4.1.60 host 10.1.17.50 eq 2000

!permit Unity to talk to Secondary CallManager
access-list 109 permit tcp host 10.4.1.60 host 10.1.17.51 eq 2000

!permit Softphone (TAPI/JTAPI) to do call setup to Primary CallManager
access-list 109 permit tcp 10.4.1.0 0.0.0.255 host 10.1.17.50 eq 2748

!permit Softphone (TAPI/JTAPI) to do call setup to Secondary CallManager
access-list 109 permit tcp 10.4.1.0 0.0.0.255 host 10.1.17.51 eq 2748

!permit Softphone to talk to Enterprise Unity to leave messages
access-list 109 permit udp 10.4.1.0 0.0.0.255 host 10.1.60.50

!permit Softphone to talk to Medium Unity to leave messages
access-list 109 permit udp 10.4.1.0 0.0.0.255 host 10.3.2.60

!permit Softphone to talk to all phones
access-list 109 permit udp 10.4.1.0 0.0.0.255 10.4.50.0 0.0.0.255
access-list 109 permit udp 10.4.1.0 0.0.0.255 10.1.5.0 0.0.0.255
access-list 109 permit udp 10.4.1.0 0.0.0.255 10.1.6.0 0.0.0.255
access-list 109 permit udp 10.4.1.0 0.0.0.255 10.1.7.0 0.0.0.255
access-list 109 permit udp 10.4.1.0 0.0.0.255 10.1.8.0 0.0.0.255
access-list 109 permit udp 10.4.1.0 0.0.0.255 10.3.1.0 0.0.0.255
access-list 109 permit udp 10.4.1.0 0.0.0.255 10.3.52.0 0.0.0.255
```

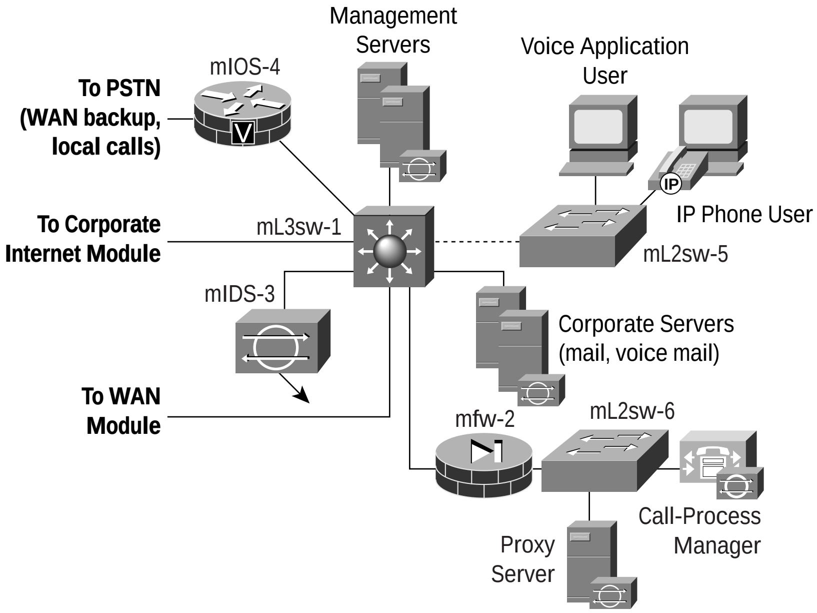
```
!permit users in the data segment to access the web server on CallManager
access-list 109 permit tcp 10.4.1.0 0.0.0.255 host 10.1.17.50 eq www

!deny all other data to voice vlan traffic/noise
access-list 109 deny   ip 10.4.1.0 0.0.0.255 10.1.17.0 0.0.0.255
access-list 109 deny   ip 10.4.1.0 0.0.0.255 10.1.60.0 0.0.0.255
access-list 109 deny   ip 10.4.1.0 0.0.0.255 host 10.3.2.60
access-list 109 deny ip 10.4.1.0 0.0.0.255 10.4.50.0 0.0.0.255
access-list 109 deny ip 10.4.1.0 0.0.0.255 10.1.7.0 0.0.0.255
access-list 109 deny ip 10.4.1.0 0.0.0.255 10.1.8.0 0.0.0.255
access-list 109 deny ip 10.4.1.0 0.0.0.255 10.3.52.0 0.0.0.255

!RFC 2827 filtering
access-list 109 permit ip 10.4.0.0 0.0.255.255 any
access-list 109 deny   ip any any log

!Access-list for Voice VLAN
!permit DHCP to router
access-list 150 permit udp host 0.0.0.0 host 255.255.255.255

!permit calls between IP phones and all phones
access-list 150 permit udp 10.4.50.0 0.0.0.255 10.4.1.0 0.0.0.255 range 16384 32767
access-list 150 permit udp 10.4.50.0 0.0.0.255 10.3.1.0 0.0.0.255 range 16384 32767
access-list 150 permit udp 10.4.50.0 0.0.0.255 10.3.52.0 0.0.0.255 range 16384 32767
access-list 150 permit udp 10.4.50.0 0.0.0.255 10.1.5.0 0.0.0.255 range 16384 32767
access-list 150 permit udp 10.4.50.0 0.0.0.255 10.1.6.0 0.0.0.255 range 16384 32767
access-list 150 permit udp 10.4.50.0 0.0.0.255 10.1.7.0 0.0.0.255 range 16384 32767
access-list 150 permit udp 10.4.50.0 0.0.0.255 10.1.8.0 0.0.0.255 range 16384 32767

!note deny at end for all other noise to phone segments
!permit IP phones to do call setup to primary CallManager
access-list 150 permit tcp 10.4.50.0 0.0.0.255 host 10.1.17.50 eq 2000

!permit IP phones to do call setup to secondary CallManager
access-list 150 permit tcp 10.4.50.0 0.0.0.255 host 10.1.17.51 eq 2000

!permit IP phones to do call setup failover with SRST on router
access-list 150 permit tcp 10.4.50.0 0.0.0.255 host 10.4.50.1 eq 2000

!permit IP phones to tftp to CallManager
access-list 150 permit udp 10.4.50.0 0.0.0.255 host 10.1.17.50 eq tftp

!permit IP phones to tftp to CallManager
access-list 150 permit udp 10.4.50.0 0.0.0.255 host 10.1.17.51 eq tftp

!note deny at end for all other noise to CM segment
!permit IP phones to leave messages on Medium Unity
access-list 150 permit udp 10.4.50.0 0.0.0.255 host 10.3.2.60 range 16384 32767

!permit IP phones to leave messages on Enterprise Unity
access-list 150 permit udp 10.4.50.0 0.0.0.255 host 10.1.60.50 range 16384 32767

!note deny at end filters out all other noise to Unity segments
access-list 150 deny   ip any any log
```

```
! The following lines are for Survivable Remote Site Telephony (SRST)
call-manager-fallback

!run SRST on a specific IP address and port
 ip source-address 10.4.50.1 port 2000
 max-ephones 48
 max-dn 192
 voicemail 4500
 call-forward busy 4500
 moh music-on-hold.au
```

Medium IP Telephony Design

Configurations for Medium Standalone Campus Module

Figure A-3
Medium Standalone Campus Module



Configuration for Layer 3 Switch: mL3sw-1

```
!addresses to exclude from dhcp – default router and broadcast
ip dhcp excluded-address 10.3.52.1
ip dhcp excluded-address 10.3.52.255

!sample static MAC to IP mapping
ip dhcp pool ip-phone-pool
   host 10.3.52.129 255.255.255.0
   client-identifier 0100.02fd.06e9.3f
   dns-server 10.3.2.50
   default-router 10.3.52.1
   domain-name safe-medium.com

! IP address of Call Manager
   option 150 ip 10.3.51.50
```

```
!data/user segment
interface Vlan10
 ip address 10.3.1.1 255.255.255.0
 ip access-group 101 in
 no ip redirects
 no cdp enable

!corporate server segment
interface Vlan11
 ip address 10.3.2.1 255.255.255.0
 ip access-group 102 in
 no ip redirects
 no cdp enable

! Call Manager firewall segment
interface Vlan50
 ip address 10.3.50.1 255.255.255.0
 ip access-group 150 in
 no cdp enable

! IP phone segment
interface Vlan52
 ip address 10.3.52.1 255.255.255.0
 ip access-group 152 in
 no cdp enable

! Management segment
interface Vlan99
 ip address 10.3.8.1 255.255.255.0
 ip access-group 103 in
 no ip redirects
 no cdp enable

! Access-list for data vlan
!permit voice between Softphone and Unity
access-list 101 permit udp 10.3.1.0 0.0.0.255 host 10.3.2.60 range 16384 32767

! deny other noise to Unity host
access-list 101 deny ip 10.3.1.0 0.0.0.255 host 10.3.2.60

!permit voice between Softphone and IP phones
access-list 101 permit udp 10.3.1.0 0.0.0.255 10.3.52.0 0.0.0.255 range 16384 32767

!filter out rest of noise to IP phones
access-list 101 deny ip 10.3.1.0 0.0.0.255 10.3.52.0 0.0.0.255

!permit Softphone (TAPI/JTAPI) call setup to CallManager
access-list 101 permit tcp 10.3.1.0 0.0.0.255 host 10.3.51.50 eq 2748

!permit users in data segment to access web server on CallManager
access-list 101 permit tcp 10.3.1.0 0.0.0.255 host 10.3.51.50 eq www

!deny all other traffic from the data segment to the CallManager segment
access-list 101 deny   ip 10.3.1.0 0.0.0.255 10.3.51.0 0.0.0.255
```

```
!RFC 2827 filtering
access-list 101 permit ip 10.3.1.0 0.0.0.255 any
access-list 101 deny   ip any any log

!Access-list for corporate server vlan
! permit voice between Unity and SoftPhone
access-list 102 permit udp host 10.3.2.60 10.3.1.0 0.0.0.255 range 16384 32767

! permit voice between Unity and IP phones
access-list 102 permit udp host 10.3.2.60 10.3.52.0 0.0.0.255 range 16384 32767

! permit HIDS agent to talk to HIDS manager console
access-list 102 permit tcp host 10.3.2.60 host 10.3.8.253 eq 5000

! permit Unity to talk to CallManager
access-list 102 permit tcp host 10.3.2.60 host 10.3.51.50 eq 2000

! RFC 2827 filtering
access-list 102 permit ip 10.3.2.0 0.0.0.255 any
access-list 102 deny   ip any any log

!Management VLAN – this is an abbreviated version, see the SAFE small, medium, and
remote design paper for the entire ACL.

!permit HIDS agent on CallManager to talk to HIDS manager console
access-list 103 permit tcp host 10.3.51.50 host 10.3.8.253 eq 5000

! permit HIDS agent on Unity to talk to HIDS manager console
access-list 103 permit tcp host 10.3.2.60 host 10.3.8.253 eq 5000

!CallManager VLAN
! permit CallManager to talk to Unity
access-list 150 permit tcp host 10.3.51.50 eq 2000 host 10.3.2.60

! permit CallManager to do call setup with IP phones
access-list 150 permit tcp host 10.3.51.50 eq 2000 10.3.52.0 0.0.0.255

!permit CallManager to allow tftp inbound from IP phones
access-list 150 permit udp host 10.3.51.50 eq tftp 10.3.52.0 0.0.0.255

!permit CallManager to allow Softphone to do call setup (TAPI/JTAPI)
access-list 150 permit tcp host 10.3.51.50 eq 2748 10.3.1.0 0.0.0.255

!permit users in the data segment to access the web server on the CallManager
access-list 150 permit tcp host 10.3.51.50 eq www 10.3.1.0 0.0.0.255

!permit the HIDS console on CallManager to talk to the HIDS management console
access-list 150 permit tcp host 10.3.51.50 host 10.3.8.253 eq 5000
access-list 150 deny   ip any any log

!IP phone VLAN, note deny at end to filter out noise
!Allow DHCP to router
access-list 152 permit udp host 0.0.0.0 host 255.255.255.255

!permit IP phones to talk skinny to CallManager
access-list 152 permit tcp 10.3.52.0 0.0.0.255 host 10.3.51.50 eq 2000
```

```
!permit IP phones to tftp their configurations from CallManager
access-list 152 permit udp 10.3.52.0 0.0.0.255 host 10.3.51.50 eq tftp

! permit IP phones to talk to SoftPhone
access-list 152 permit udp 10.3.52.0 0.0.0.255 10.3.1.0 0.0.0.255 range 16384 32767

!permit IP phones to leave messages on Unity
access-list 152 permit udp 10.3.52.0 0.0.0.255 host 10.3.2.60 range 16384 32767
access-list 152 deny   ip any any log
```

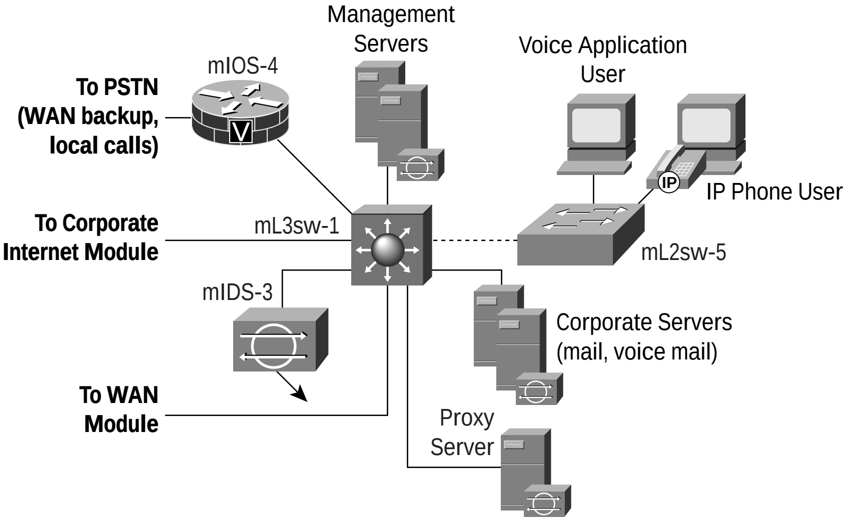
Configuration for Stateful Firewall: mfw-2

```
!note implicit deny at end to filter out noise
ip address outside 10.3.50.2 255.255.255.0
ip address inside 10.3.51.1 255.255.255.0

!static IP address translation (NAT 0) for CallManager
static (inside,outside) 10.3.51.50 10.3.51.50 netmask 255.255.255.255 0 0

!access-control inbound
access-group out in interface outside

!permit SoftPhone to connect to the CallManager for call setup
access-list out permit tcp 10.3.1.0 255.255.255.0 host 10.3.51.50 eq 2748

!permit IP Phones to connect to CallManager for call setup
access-list out permit tcp 10.3.52.0 255.255.255.0 host 10.3.51.50 eq 2000

!permit IP phones to connect to CallManager for configurations via TFTP
access-list out permit udp 10.3.52.0 255.255.255.0 host 10.3.51.50 eq tftp

!permit Unity to contact CallManager for voicemail
access-list out permit tcp host 10.3.2.60 host 10.3.51.50 eq 2000
```

Configurations for Medium Branch Corporate Internet Module

Figure A-4

Medium Branch Campus Module



Configuration for Layer 3 Switch: mL3sw-1

```
!addresses to exclude from dhcp – default router and broadcast
ip dhcp excluded-address 10.3.52.1
ip dhcp excluded-address 10.3.52.255

!sample static MAC to IP mapping
ip dhcp pool ip-phone-pool
   host 10.3.52.129 255.255.255.0
   client-identifier 0100.02fd.06e9.3f
   dns-server 10.3.2.50
   default-router 10.3.52.1
   domain-name safe-medium.com

! IP address of Call Manager
   option 150 ip 10.1.17.50

!data/user segment
interface Vlan10
 ip address 10.3.1.1 255.255.255.0
 ip access-group 101 in
 no ip redirects
 no cdp enable

!corporate server segment
interface Vlan11
 ip address 10.3.2.1 255.255.255.0
 ip access-group 102 in
 no ip redirects
 no cdp enable

! Call Manager firewall segment
interface Vlan52
```

```
 ip address 10.3.52.1 255.255.255.0
 ip access-group 152 in
 no cdp enable

! Management segment
interface Vlan99
 ip address 10.3.8.1 255.255.255.0
 ip access-group 103 in
 no ip redirects
 no cdp enable

! Access-list for data vlan
!permit voice between Softphone and Medium Unity
access-list 101 permit udp 10.3.1.0 0.0.0.255 host 10.3.2.60 range 16384 32767

!permit voice between Softphone and Large Unity
access-list 101 permit udp 10.3.1.0 0.0.0.255 host 10.1.60.50 range 16384 32767

!filter out noise to Unity segments
access-list 101 deny ip 10.3.1.0 0.0.0.255 host 10.3.2.60
access-list 101 deny ip 10.3.1.0 0.0.0.255 10.1.60.0 0.0.0.255

!permit voice between Softphone and all phones
access-list 101 permit udp 10.3.1.0 0.0.0.255 10.3.52.0 0.0.0.255 range 16384 32767
access-list 101 permit udp 10.3.1.0 0.0.0.255 10.1.5.0 0.0.0.255 range 16384 32767
access-list 101 permit udp 10.3.1.0 0.0.0.255 10.1.6.0 0.0.0.255 range 16384 32767
access-list 101 permit udp 10.3.1.0 0.0.0.255 10.1.7.0 0.0.0.255 range 16384 32767
access-list 101 permit udp 10.3.1.0 0.0.0.255 10.1.8.0 0.0.0.255 range 16384 32767
access-list 101 permit udp 10.3.1.0 0.0.0.255 10.4.1.0 0.0.0.255 range 16384 32767
access-list 101 permit udp 10.3.1.0 0.0.0.255 10.4.50.0 0.0.0.255 range 16384 32767

!filter out all noise to voice networks
access-list 101 deny ip 10.3.1.0 0.0.0.255 10.3.52.0 0.0.0.255
access-list 101 deny ip 10.3.1.0 0.0.0.255 10.1.7.0 0.0.0.255
access-list 101 deny ip 10.3.1.0 0.0.0.255 10.1.8.0 0.0.0.255
access-list 101 deny ip 10.3.1.0 0.0.0.255 10.4.50.0 0.0.0.255

!permit Softphone (TAPI/JTAPI) call setup to primary CallManager
access-list 101 permit tcp 10.3.1.0 0.0.0.255 host 10.1.17.50 eq 2748

!permit Softphone (TAPI/JTAPI) call setup to secondary CallManager
access-list 101 permit tcp 10.3.1.0 0.0.0.255 host 10.1.17.51 eq 2748

!permit users in data network to access web server on primary CallManager only
access-list 101 permit tcp 10.3.1.0 0.0.0.255 host 10.1.17.50 eq www

!deny all other traffic from the data segment to the CallManager segment
access-list 101 deny   ip 10.3.1.0 0.0.0.255 10.1.17.0 0.0.0.255

!RFC 2827 filtering
access-list 101 permit ip 10.3.1.0 0.0.0.255 any
access-list 101 deny   ip any any log
```

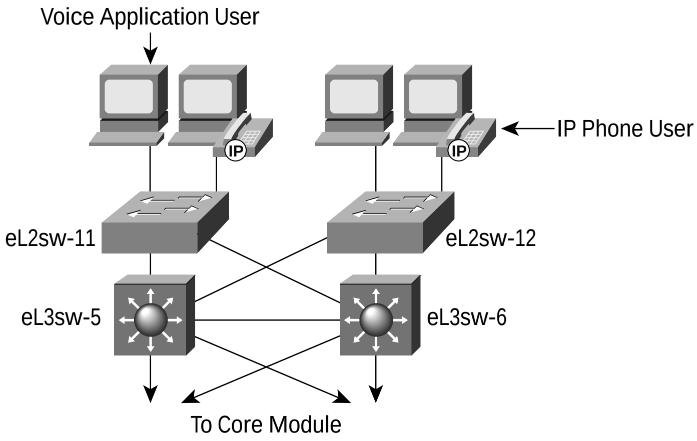
```
!Access-list for corporate server vlan
!permit voice between Unity and phones for leaving messages
access-list 102 permit udp host 10.3.2.60 10.3.1.0 0.0.0.255 range 16384 32767
access-list 102 permit udp host 10.3.2.60 10.3.52.0 0.0.0.255 range 16384 32767
access-list 102 permit udp host 10.3.2.60 10.4.1.0 0.0.0.255 range 16384 32767
access-list 102 permit udp host 10.3.2.60 10.4.50.0 0.0.0.255 range 16384 32767
access-list 102 permit udp host 10.3.2.60 10.1.5.0 0.0.0.255 range 16384 32767
access-list 102 permit udp host 10.3.2.60 10.1.6.0 0.0.0.255 range 16384 32767
access-list 102 permit udp host 10.3.2.60 10.1.7.0 0.0.0.255 range 16384 32767
access-list 102 permit udp host 10.3.2.60 10.1.8.0 0.0.0.255 range 16384 32767

!deny all other noise
access-list 102 deny ip host 10.3.2.60 10.3.1.0 0.0.0.255
access-list 102 deny ip host 10.3.2.60 10.3.52.0 0.0.0.255
access-list 102 deny ip host 10.3.2.60 10.4.1.0 0.0.0.255
access-list 102 deny ip host 10.3.2.60 10.4.50.0 0.0.0.255
access-list 102 deny ip host 10.3.2.60 10.1.5.0 0.0.0.255
access-list 102 deny ip host 10.3.2.60 10.1.6.0 0.0.0.255
access-list 102 deny ip host 10.3.2.60 10.1.7.0 0.0.0.255
access-list 102 deny ip host 10.3.2.60 10.1.8.0 0.0.0.255

! permit HIDS agent to talk to HIDS manager console
access-list 102 permit tcp host 10.3.2.60 host 10.3.8.253 eq 5000

! permit Unity to talk to primary CallManager
access-list 102 permit tcp host 10.3.2.60 host 10.1.17.50 eq 2000

! permit Unity to talk to secondary CallManager
access-list 102 permit tcp host 10.3.2.60 host 10.1.17.51 eq 2000

!deny other noise sent to CM segment
access-list 102 deny ip host 10.3.2.60 10.1.17.0 0.0.0.255

! RFC 2827 filtering
access-list 102 permit ip 10.3.2.0 0.0.0.255 any
access-list 102 deny   ip any any log

!Management VLAN – this is an abbreviated version, see the SAFE small, medium, and
remote design paper for the entire ACL.

!permit HIDS agent on CallManager to talk to HIDS manager console
access-list 103 permit tcp host 10.3.51.50 host 10.3.8.253 eq 5000

! permit HIDS agent on Unity to talk to HIDS manager console
access-list 103 permit tcp host 10.3.2.60 host 10.3.8.253 eq 5000

!IP phone VLAN, note deny at end to filter out all noise
!Allow DHCP to router
access-list 152 permit udp host 0.0.0.0 host 255.255.255.255

!permit IP phones to do call setup to primary CallManager
access-list 152 permit tcp 10.3.52.0 0.0.0.255 host 10.1.17.50 eq 2000

!permit IP phones to do call setup to secondary CallManager
access-list 152 permit tcp 10.3.52.0 0.0.0.255 host 10.1.17.51 eq 2000
```

```
!permit IP phones to tftp their configurations from primary CallManager
access-list 152 permit udp 10.3.52.0 0.0.0.255 host 10.1.17.50 eq tftp

!permit IP phones to tftp their configurations from secondary CallManager
access-list 152 permit udp 10.3.52.0 0.0.0.255 host 10.1.17.51 eq tftp

! permit IP phones to talk to all phones
access-list 152 permit udp 10.3.52.0 0.0.0.255 10.3.1.0 0.0.0.255 range 16384 32767
access-list 152 permit udp 10.3.52.0 0.0.0.255 10.4.1.0 0.0.0.255 range 16384 32767
access-list 152 permit udp 10.3.52.0 0.0.0.255 10.4.50.0 0.0.0.255 range 16384 32767
access-list 152 permit udp 10.3.52.0 0.0.0.255 10.1.5.0 0.0.0.255 range 16384 32767
access-list 152 permit udp 10.3.52.0 0.0.0.255 10.1.6.0 0.0.0.255 range 16384 32767
access-list 152 permit udp 10.3.52.0 0.0.0.255 10.1.7.0 0.0.0.255 range 16384 32767
access-list 152 permit udp 10.3.52.0 0.0.0.255 10.1.8.0 0.0.0.255 range 16384 32767

!permit IP phones to leave messages on Medium Unity
access-list 152 permit udp 10.3.52.0 0.0.0.255 host 10.3.2.60 range 16384 32767

!permit IP phones to leave messages on Enterprise Unity
access-list 152 permit udp 10.3.52.0 0.0.0.255 host 10.1.60.50 range 16384 32767

!deny all other noise
access-list 152 deny   ip any any log
```

Enterprise IP Telephony Design

Configurations for Building Module

Figure A-5
Large Enterprise Voice Building Module



Configuration for Layer 3 Switch: eL3sw-5

```
!DHCP addresses to exclude – router and broadcast
ip dhcp excluded-address 10.1.8.1 10.1.8.1
ip dhcp excluded-address 10.1.8.1 10.1.8.255

!sample DHCP IP address assignment tied to known MAC
ip dhcp pool ip-phone-pool-1
   host 10.1.8.129 255.255.255.0
   client-identifier 0100.3094.c263.58
   dns-server 10.1.11.50
   default-router 10.1.8.5
   domain-name safe-enterprise.com

!IP address of CallManager
   option 150 ip 10.1.17.50

! Marketing Data VLAN
interface Vlan5
 ip address 10.1.5.5 255.255.255.0
 ip access-group 105 in
 no cdp enable

!R&D Data VLAN
interface Vlan6
 ip address 10.1.6.5 255.255.255.0
 ip access-group 106 in
 no cdp enable

!Marketing IP Phone VLAN
interface Vlan7
 ip address 10.1.7.5 255.255.255.0
 ip access-group 107 in
 no cdp enable

!R&D IP Phone VLAN
interface Vlan8
 ip address 10.1.8.5 255.255.255.0
 ip access-group 108 in
 no cdp enable

!Access-list for marketing data network
!permit Softphone to do call setup with the primary CallManager
access-list 105 permit tcp 10.1.5.0 0.0.0.255 host 10.1.17.50 eq 2748

!permit Softphone to do call setup with the secondary CallManager
access-list 105 permit tcp 10.1.5.0 0.0.0.255 host 10.1.17.51 eq 2748

!permit data users to access the web server on the primary CallManager
access-list 105 permit tcp 10.1.5.0 0.0.0.255 host 10.1.17.50 eq www

!deny all other traffic to call manager segment
access-list 105 deny   ip 10.1.5.0 0.0.0.255 10.1.17.0 0.0.0.255

!permit Softphone to send voice to Enterprise Unity to leave message
access-list 105 permit udp 10.1.5.0 0.0.0.255 host 10.1.60.50 range 16384 32767
```

```
!permit Softphone to send voice to Medium Unity to leave message
access-list 105 permit udp 10.1.5.0 0.0.0.255 host 10.3.2.60 range 16384 32767

!deny all other traffic from softphones to Unity segments
access-list 105 deny   ip 10.1.5.0 0.0.0.255 10.1.60.0 0.0.0.255
access-list 105 deny   ip 10.1.5.0 0.0.0.255 host 10.3.2.60

!permit SoftPhone to talk to all phones in voice segments
access-list 105 permit udp 10.1.5.0 0.0.0.255 10.1.7.0 0.0.0.255 range 16384 32767
access-list 105 permit udp 10.1.5.0 0.0.0.255 10.1.8.0 0.0.0.255 range 16384 32767
access-list 105 permit udp 10.1.5.0 0.0.0.255 10.4.50.0 0.0.0.255 range 16384 32767
access-list 105 permit udp 10.1.5.0 0.0.0.255 10.3.52.0 0.0.0.255 range 16384 32767

!deny all other noise
access-list 105 deny ip 10.1.5.0 0.0.0.255 10.1.7.0 0.0.0.255
access-list 105 deny ip 10.1.5.0 0.0.0.255 10.1.8.0 0.0.0.255
access-list 105 deny ip 10.1.5.0 0.0.0.255 10.4.50.0 0.0.0.255
access-list 105 deny ip 10.1.5.0 0.0.0.255 10.3.52.0 0.0.0.255

!RFC 2827 filtering
access-list 105 permit ip 10.1.5.0 0.0.0.255 any
access-list 105 deny   ip any any log

!Access-list for R&D data network
!permit Softphone to do call setup with the primary CallManager
access-list 106 permit tcp 10.1.6.0 0.0.0.255 host 10.1.17.50 eq 2748

!permit Softphone to do call setup with the secondary CallManager
access-list 106 permit tcp 10.1.6.0 0.0.0.255 host 10.1.17.51 eq 2748

!permit data users to access the web server on the primary CallManager
access-list 106 permit tcp 10.1.6.0 0.0.0.255 host 10.1.17.50 eq www

!deny all other traffic to call manager segment
access-list 106 deny   ip 10.1.6.0 0.0.0.255 10.1.17.0 0.0.0.255

!permit Softphone to send voice to Enterprise Unity to leave message
access-list 106 permit udp 10.1.6.0 0.0.0.255 host 10.1.60.50

!permit Softphone to send voice to Medium Unity to leave message
access-list 106 permit udp 10.1.6.0 0.0.0.255 host 10.3.2.60

!deny all other traffic from softphones to Unity segments
access-list 106 deny   ip 10.1.6.0 0.0.0.255 10.1.60.0 0.0.0.255
access-list 106 deny   ip 10.1.6.0 0.0.0.255 host 10.3.2.60

!permit SoftPhone to talk to all phones in voice segments
access-list 106 permit udp 10.1.6.0 0.0.0.255 10.1.7.0 0.0.0.255 range 16384 32767
access-list 106 permit udp 10.1.6.0 0.0.0.255 10.1.8.0 0.0.0.255 range 16384 32767
access-list 106 permit udp 10.1.6.0 0.0.0.255 10.4.50.0 0.0.0.255 range 16384 32767
access-list 106 permit udp 10.1.6.0 0.0.0.255 10.3.52.0 0.0.0.255 range 16384 32767

!deny all other noise
access-list 106 deny ip 10.1.6.0 0.0.0.255 10.1.7.0 0.0.0.255
access-list 106 deny ip 10.1.6.0 0.0.0.255 10.1.8.0 0.0.0.255
access-list 106 deny ip 10.1.6.0 0.0.0.255 10.4.50.0 0.0.0.255
access-list 106 deny ip 10.1.6.0 0.0.0.255 10.3.52.0 0.0.0.255
```

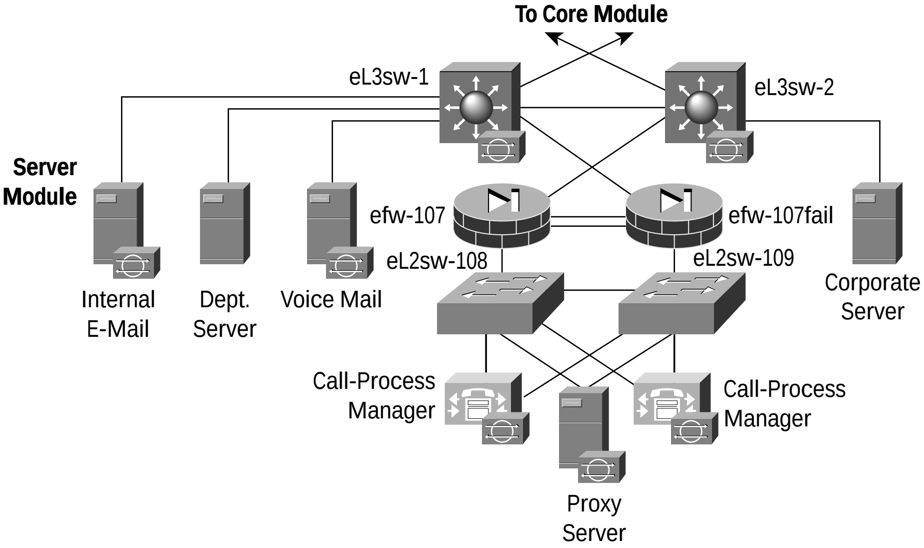
```
!RFC 2827 filtering
access-list 106 permit ip 10.1.6.0 0.0.0.255 any
access-list 106 deny   ip any any log

!Access-list for Marketing Voice network, note deny at end
!permit DHCP to router
access-list 107 permit udp host 0.0.0.0 host 255.255.255.255

!permit IP phones to leave messages on Enterprise Unity
access-list 107 permit udp 10.1.7.0 0.0.0.255 host 10.1.60.50 range 16384 32767

!permit IP phones to leave messages on Medium Unity
access-list 107 permit udp 10.1.7.0 0.0.0.255 host 10.3.2.60 range 16384 32767

!permit IP phones to talk to all other phones
!note deny at end to filter out noise
access-list 107 permit udp 10.1.7.0 0.0.0.255 10.1.5.0 0.0.0.255 range 16384 32767
access-list 107 permit udp 10.1.7.0 0.0.0.255 10.1.6.0 0.0.0.255 range 16384 32767
access-list 107 permit udp 10.1.7.0 0.0.0.255 10.1.8.0 0.0.0.255 range 16384 32767
access-list 107 permit udp 10.1.7.0 0.0.0.255 10.3.1.0 0.0.0.255 range 16384 32767
access-list 107 permit udp 10.1.7.0 0.0.0.255 10.3.52.0 0.0.0.255 range 16384 32767
access-list 107 permit udp 10.1.7.0 0.0.0.255 10.1.70.0 0.0.0.255 range 16384 32767
access-list 107 permit udp 10.1.7.0 0.0.0.255 10.4.1.0 0.0.0.255 range 16384 32767
access-list 107 permit udp 10.1.7.0 0.0.0.255 10.4.50.0 0.0.0.255 range 16384 32767

!note deny at end for all other noise
!permit IP Phones to do call setup and configuration retrieval with CallManager
access-list 107 permit tcp 10.1.7.0 0.0.0.255 host 10.1.17.50 eq 2000
access-list 107 permit tcp 10.1.7.0 0.0.0.255 host 10.1.17.51 eq 2000
access-list 107 permit udp 10.1.7.0 0.0.0.255 host 10.1.17.50 eq tftp
access-list 107 permit udp 10.1.7.0 0.0.0.255 host 10.1.17.51 eq tftp

!note next deny for rest of noise
access-list 107 deny   ip any any log

!Access-list for R&D Voice network, note deny at end
!permit DHCP to router
access-list 108 permit udp host 0.0.0.0 host 255.255.255.255

!permit IP phones to leave messages on Enterprise Unity
access-list 108 permit udp 10.1.8.0 0.0.0.255 host 10.1.60.50 range 16384 32767

!permit IP phones to leave messages on Medium Unity
access-list 108 permit udp 10.1.8.0 0.0.0.255 host 10.3.2.60 range 16384 32767

!permit IP phones to talk to all other phones
access-list 108 permit udp 10.1.8.0 0.0.0.255 10.1.5.0 0.0.0.255 range 16384 32767
access-list 108 permit udp 10.1.8.0 0.0.0.255 10.1.6.0 0.0.0.255 range 16384 32767
access-list 108 permit udp 10.1.8.0 0.0.0.255 10.1.7.0 0.0.0.255 range 16384 32767
access-list 108 permit udp 10.1.8.0 0.0.0.255 10.3.1.0 0.0.0.255 range 16384 32767
access-list 108 permit udp 10.1.8.0 0.0.0.255 10.3.52.0 0.0.0.255 range 16384 32767
access-list 108 permit udp 10.1.8.0 0.0.0.255 10.1.70.0 0.0.0.255 range 16384 32767
access-list 108 permit udp 10.1.8.0 0.0.0.255 10.4.1.0 0.0.0.255 range 16384 32767
access-list 108 permit udp 10.1.8.0 0.0.0.255 10.4.50.0 0.0.0.255 range 16384 32767
```

```
!note deny at end for all other noise
!permit IP Phones to do call setup and configuration retrieval with CallManager
access-list 108 permit tcp 10.1.8.0 0.0.0.255 host 10.1.17.50 eq 2000
access-list 108 permit tcp 10.1.8.0 0.0.0.255 host 10.1.17.51 eq 2000
access-list 108 permit udp 10.1.8.0 0.0.0.255 host 10.1.17.50 eq tftp
access-list 108 permit udp 10.1.8.0 0.0.0.255 host 10.1.17.51 eq tftp

!note next deny for rest of noise
access-list 108 deny   ip any any log
```

Configurations for Server Module

Figure A-6

Large Enterprise Server Module



Configuration for Layer 3 Switch: eL3sw-2

```
! CallManager segment
interface Vlan16
 ip address 10.1.16.2 255.255.255.0
 ip access-group 116 in
 no ip redirects
 no cdp enable
 standby 1 priority 50 preempt
 standby 1 ip 10.1.16.100
 standby 1 track Vlan23
 standby 1 track Vlan24

!Unity Segment
interface Vlan60
 ip address 10.1.60.2 255.255.255.0
 ip access-group 160 in
 no ip redirects
 no cdp enable
 standby 1 priority 50 preempt
 standby 1 ip 10.1.60.100
 standby 1 track Vlan23
 standby 1 track Vlan24
```

```
access-list 116 permit tcp host 10.1.17.50 host 10.1.20.151 eq 5000

!permit Enterprise Unity connections to CallManager
access-list 116 permit tcp host 10.1.17.50 eq 2000 host 10.1.60.50

!permit Softphone to connect to CallManager for call setup
access-list 116 permit tcp host 10.1.17.50 eq 2748 10.1.5.0 0.0.0.255
access-list 116 permit tcp host 10.1.17.50 eq 2748 10.1.6.0 0.0.0.255
access-list 116 permit tcp host 10.1.17.50 eq 2748 10.3.1.0 0.0.0.255
access-list 116 permit tcp host 10.1.17.50 eq 2748 10.3.4.0 0.0.0.255

!permit IP Phones to connect to CallManager for call setup and configurations
access-list 116 permit tcp host 10.1.17.50 eq 2000 10.1.7.0 0.0.0.255
access-list 116 permit tcp host 10.1.17.50 eq 2000 10.1.8.0 0.0.0.255
access-list 116 permit tcp host 10.1.17.50 eq 2000 10.3.52.0 0.0.0.255
access-list 116 permit tcp host 10.1.17.50 eq 2000 10.4.50.0 0.0.0.255
access-list 116 permit udp host 10.1.17.50 eq tftp 10.1.7.0 0.0.0.255
access-list 116 permit udp host 10.1.17.50 eq tftp 10.1.8.0 0.0.0.255
access-list 116 permit udp host 10.1.17.50 eq tftp 10.3.52.0 0.0.0.255
access-list 116 permit udp host 10.1.17.50 eq tftp 10.4.50.0 0.0.0.255

!comments same as above now for secondary unit
access-list 116 permit tcp host 10.1.17.51 host 10.1.20.151 eq 5000
access-list 116 permit tcp host 10.1.17.51 eq 2000 host 10.1.60.50
access-list 116 permit tcp host 10.1.17.51 eq 2748 10.1.5.0 0.0.0.255
access-list 116 permit tcp host 10.1.17.51 eq 2748 10.1.6.0 0.0.0.255
access-list 116 permit tcp host 10.1.17.51 eq 2748 10.3.1.0 0.0.0.255
access-list 116 permit tcp host 10.1.17.51 eq 2748 10.3.4.0 0.0.0.255
access-list 116 permit tcp host 10.1.17.51 eq 2000 10.1.7.0 0.0.0.255
access-list 116 permit tcp host 10.1.17.51 eq 2000 10.1.8.0 0.0.0.255
access-list 116 permit tcp host 10.1.17.51 eq 2000 10.3.52.0 0.0.0.255
access-list 116 permit tcp host 10.1.17.51 eq 2000 10.4.50.0 0.0.0.255
access-list 116 permit udp host 10.1.17.51 eq tftp 10.1.7.0 0.0.0.255
access-list 116 permit udp host 10.1.17.51 eq tftp 10.1.8.0 0.0.0.255
access-list 116 permit udp host 10.1.17.51 eq tftp 10.3.52.0 0.0.0.255
access-list 116 permit udp host 10.1.17.51 eq tftp 10.4.50.0 0.0.0.255
access-list 116 permit udp host 10.1.16.1 host 224.0.0.2 eq 1985
access-list 116 deny   ip any any log

!Access control for Unity segment, note deny at end for all noise
!permit HIDS agent on Unity to contact HIDS manger in Management module
access-list 160 permit tcp host 10.1.60.50 host 10.1.20.151 eq 5000

!permit Unity to connect to CallManager for voicemail notifications
access-list 160 permit tcp host 10.1.60.50 host 10.1.17.50 eq 2000
access-list 160 permit tcp host 10.1.60.50 host 10.1.17.51 eq 2000

!permit all phones to connect to Unity to leave voicemail messages
access-list 160 permit udp host 10.1.60.50 10.1.5.0 0.0.0.255 range 16384 32767
access-list 160 permit udp host 10.1.60.50 10.1.6.0 0.0.0.255 range 16384 32767
access-list 160 permit udp host 10.1.60.50 10.1.7.0 0.0.0.255 range 16384 32767
access-list 160 permit udp host 10.1.60.50 10.1.8.0 0.0.0.255 range 16384 32767
access-list 160 permit udp host 10.1.60.50 10.1.70.0 0.0.0.255 range 16384 32767
access-list 160 permit udp host 10.1.60.50 10.3.52.0 0.0.0.255 range 16384 32767
access-list 160 permit udp host 10.1.60.50 10.3.70.0 0.0.0.255 range 16384 32767
access-list 160 permit udp host 10.1.60.50 10.3.1.0 0.0.0.255 range 16384 32767
```

```
access-list 160 permit udp host 10.1.60.50 10.4.50.0 0.0.0.255 range 16384 32767
access-list 160 permit udp host 10.1.60.50 10.4.1.0 0.0.0.255 range 16384 32767
access-list 160 deny   ip any any log
```

Configuration for Stateful Firewall: efw-107

```
!note implicit deny at end to filter out noise
ip address outside 10.1.16.3 255.255.255.0
ip address inside 10.1.17.1 255.255.255.0

!static translation (NAT 0) for CallManager
static (inside,outside) 10.1.17.50 10.1.17.50 netmask 255.255.255.255 0 0

!access control applied inbound
access-group out in interface outside

!permit IP Phones to connect to CallManager for call setup and configuration
access-list out permit tcp 10.3.54.0 255.255.255.0 host 10.1.17.50 eq 2000
access-list out permit udp 10.3.54.0 255.255.255.0 host 10.1.17.50 eq tftp
access-list out permit tcp 10.1.8.0 255.255.255.0 host 10.1.17.50 eq 2000
access-list out permit udp 10.1.8.0 255.255.255.0 host 10.1.17.50 eq tftp
access-list out permit tcp 10.1.7.0 255.255.255.0 host 10.1.17.50 eq 2000
access-list out permit udp 10.1.7.0 255.255.255.0 host 10.1.17.50 eq tftp

!permit SoftPhone to connect to CallManager for call setup
access-list out permit tcp 10.1.6.0 255.255.255.0 host 10.1.17.50 eq 2748
access-list out permit tcp 10.1.5.0 255.255.255.0 host 10.1.17.50 eq 2748

!permit Unity to connect to CallManager for voicemail notification
access-list out permit tcp host 10.1.60.50 host 10.1.17.50 eq 2000
```

Appendix B: IP Telephony Primer

The Need for IP Telephony

The convergence of voice and data traffic on a single IP network is revolutionizing communications. Voice can now be transported as high-priority data, lowering the cost of network ownership and enhancing business communications via the enablement of value-added applications. Many of the new business applications that are now deployed on converged networks provide immediate ways to increase personal and workgroup productivity, while enhancing customer care and responsiveness.

IP Telephony Network Components

There are four main voice-specific components of a IP telephony network:

- *IP telephony devices:* This refers to any device that supports placing calls in an IP telephony network. IP phones are included as well as applications installed on user systems with speakers and microphones. IP phones offer services such as user directory lookups and Internet access for stock quotes; these are referred to as IP phone services and are accessed via a proxy server.
- *Call-processing manager:* This server provides call control and configuration management for IP telephony devices; also known as "IP PBX." This device provides the core functionality to bootstrap IP telephony devices, provide call setup, and route calls throughout the network to other voice devices including voice gateways and voice-mail systems.
- *Voice-mail system:* Provides IP-based voice-mail storage and an autoattendant (an automated attendant providing voice services) for services such as user directory lookup and call forwarding.
- *Voice gateway:* A general term used to refer to any gateway that provides voice services including such features as PSTN access, IP packet routing, backup call-processing, and voice services. This is the device that provides access to legacy voice systems for local calls, toll bypass, and WAN backup in case of failure. Backup call processing allows for the voice gateway to take over call processing in case the primary call-processing manager goes offline for any reason. Typically the voice gateway supports a subset of the call-processing functionality supported by the call-processing manager.

IP Telephony Component Interactions: A Working Example With The Skinny Station Protocol

The IP telephony component interactions listed below model that of the Skinny Station Protocol and are provided as a reference call setup flow.

The initial step all IP telephony devices must complete before placing a call is possible is call-processing manager registration. For the Cisco skinny protocol this process occurs over TCP/2748 (control channel) and UDP/69 (trivial file transfer protocol (TFTP) for phone configuration and firmware updates). At the end of this step, the IP telephony devices are configured with access to voice-mail, data services, time-of-day, speed-dials, any other custom configurations, and an extension. If voice-mail was pending the message waiting indicator light will illuminate. If the device is an IP phone and there is new OS code available, it will download the code, install it, reboot, and restart the registration process. An open connection is maintained at all times between the IP telephony device and the call-processing manager. This can be used for instance to notify the IP telephony device if a voice-mail was received and to ensure a call-process manager is always available for call processing.

At this point the device is ready to place a call. Once the user dials the extension of the remote user they want to talk to, the extension is sent to the call-processing manager which then in turn notifies the destination device that a call is incoming. Because the destination device went through the registration process, the call-processing manager will be able to fulfill the call. Once the remote user takes the device off-hook, the remote device notifies the call-processing manager that it is willing to accept the call. At this point the call-processing manager notifies both devices that a channel is now available for them to converse over.

This channel uses the Real Time Protocol (RTP) running on top of UDP/IP to allow the conversation to commence. The UDP stream originates on the calling IP phone and terminates on the target IP phone; the call-process manager does not access the stream. For information about how the caller's voices are converted into UDP datagrams see the voice transport basics section later in this appendix. Once one party hangs up the call-processing manager notifies the other side and the UDP session is torn down. If the remote user had been unavailable, the call-processing manager would have instead established an RTP session with the voice-mail server. At that time the user could then leave a voice-mail message.

One other interaction is worth mentioning. IP phones support dynamic content services via an HTTP client and Extensible Markup Language (XML) support. The IP phone contains a service locator that is responsibile for contacting the call-process manager to determine what authorized services are available. When a service is accessed on the IP phone, it creates an HTTP connection to the proxy server. Once the list of services is determined, the phone then creates another HTTP connection to the call-processing manager. In this connection request is included the phone's identification (MAC address). This allows the call-processing manager to check what services the phone has enabled and then notifies the phone.

At this point the services available to the user are displayed on the phone. If the user chooses for instance a stock quote, the request is sent to the proxy server over HTTP to fulfill the request. The proxy server then establishes its own HTTP connection outbound to retrieve the stock's price, records the result, and finally sends the result back to the phone at which time it is displayed to the user.

IP Telephony Deployment Models

There are three main models for the deployment of enterprise IP telephony networks:

- *Single-site campus*—This is the most basic deployment scenario in which all IP telephony devices reside in a single campus (covered in SAFE IP telephony security in depth).
- *WAN centralized call-processing*—This is a moderately complex scenario in which multiple sites are connected over a private WAN and the headend site contains the only call-processing manager cluster. Remote sites may have voice services such as voice-mail (covered in SAFE IP telephony security in depth).
- *WAN distributed call-processing*—This is the most complex scenario in which multiple sites are connected over a private WAN and one or more of the sites contains a call-processing manager cluster. Many of the sites will also have voice services such as voice-mail (not covered in SAFE IP telephony security in depth).

Voice-over-IP (VoIP) Protocols

The three front-running proposed standards are H323, Session Initiation Protocol (SIP), and Media Gateway Control Protocol (MGCP). They are provided here for reference in addition to the Skinny flow description provided earlier.

H.323

The H.323 standard is a logical extension of the H.320 standard to enable corporate intranets and packet-switched networks to transport multimedia and conference traffic. H.323 recommendations cover the IP devices that participate and control H.323 sessions and the elements that interact with the switched-circuit network (SCN). H.323 standards do not include the LAN itself, nor the transport layer that interconnects LAN segments. In common with other International Telecommunication Union (ITU) multimedia teleconferencing standards, H.323 implementation applies to either point-to-point or multipoint sessions. The H.323 recommendation allows multipoint conferences through a variety of methods or configurations. The recommendation allows for either centralized or decentralized conference technologies.

The ITU has ratified the following core components:

- H.225—Specifies messages for call control, including signaling, registration and admissions, and packetization/ synchronization of media streams
- H.245—Specifies messages for opening and closing channels for media streams and other commands, requests, and indications
- H.261—Video codec for audiovisual services at P x 64 kbps
- H.263—Specification for a new video codec for video basic telephone service
- G.711—Audio codec, 3.1 kHz at 48, 56, and 64 kbps (normal telephony)
- G.722—Audio codec, 7 kHz at 48, 56, and 64 kbps
- G.728—Audio codec, 3.1 kHz at 16 kbps
- G.723—Audio codec for 5.3- and 6.3-kbps modes
- G.729—Audio codec

Ports or sockets used for H.245 signaling, audio, video, or data channels are dynamically negotiated between endpoints. This use of dynamic sockets makes it difficult to implement security, policy, and traffic shaping. H.323 data conferencing uses both “reliable” and “unreliable” communications. Reliable transport is for control signals and data, because signals must be received in proper order and cannot be lost. Unreliable transport is used for audio and video streams, which are time sensitive. Delayed audio and video packets are dropped. Consequently, TCP is applied to the H.245 control channel, the T.120 data channels, and the call-signaling channel, whereas User Datagram Protocol (UDP) applies to audio, video, and Registration/Authorization/Status (RAS) channels.

Because H.323-compliant applications use dynamically allocated sockets for audio, video, and data channels, a firewall must be able to allow H.323 traffic through on an intelligent basis. The firewall must be either H.323 enabled with an H.323 proxy, or it must be able to “snoop” the control channel to determine which dynamic sockets are in use for H.323 sessions, and allow traffic as long as the control channel is active.

SIP

Session Initiation Protocol (SIP) is the IETF’s standard for multimedia conferencing over IP. SIP is an ASCII-encoded, application-layer control protocol (defined in RFC 2543) that can be used to establish, maintain, and terminate calls between two or more endpoints. Like other voice-over-IP (VoIP) protocols, SIP is designed to address the functions of signaling and session management within a packet telephony network. Signaling allows call information to be carried across network boundaries. Session management provides the ability to control the attributes of an end-to-end call.

SIP provides the capabilities to:

- Determine the location of the target endpoint—SIP supports address resolution, name mapping, and call redirection.
- Determine the media capabilities of the target endpoint—Via Session Description Protocol (SDP), SIP determines the “lowest level” of common services between the endpoints. Conferences are established using only the media capabilities that can be supported by all endpoints.
- Determine the availability of the target endpoint—If a call cannot be completed because the target endpoint is unavailable, SIP determines whether the called party is already on the phone or did not answer in the allotted number of rings. It then returns a message indicating why the target endpoint was unavailable.
- Establish a session between the originating and target endpoint—If the call can be completed, SIP establishes a session between the endpoints. SIP also supports mid-call changes, such as the addition of another endpoint to the conference or the changing of a media characteristic or codec.
- Handle the transfer and termination of calls—SIP supports the transfer of calls from one endpoint to another. During a call transfer, SIP simply establishes a session between the transferee and a new endpoint (specified by the transferring party) and terminates the session between the transferee and the transferring party. At the end of a call, SIP terminates the sessions between all parties.
- Conferences can consist of two or more users and can be established using multicast or multiple unicast sessions.

Users in a SIP network are identified by unique SIP addresses. A SIP address is similar to an e-mail address and is in the format of sip:*userID@gateway.com*. The user ID can be either a username or an E.164 address. Users register with a registrar server using their assigned SIP addresses. The registrar server provides this information to the location server upon request. When a user initiates a call, a SIP request is sent to a SIP server (either a proxy or a redirect server). The request includes the address of the caller (in the From header field) and the address of the intended callee (in the To header field). The following sections provide simple examples of successful, point-to-point calls established using a proxy and a redirect server.

MGCP

In Media Gateway Control Protocol (MGCP), media gateway controllers or call agents provide control, signaling, and the processing skills to control the telephony gateways. One of the goals of MGCP is simplicity. A telephony gateway is a network device that provides conversion between the audio signals carried on telephone circuits and data packets carried on packet networks. MGCP assumes a call-control architecture wherein the call-control “intelligence” is outside the gateways and is handled by external call-control elements. MGCP is a master/slave protocol, wherein the gateways execute the commands sent by the call agents. The call agent implements the signaling layers of H.323 (listed earlier in the H.323 section) and appears to H.323 devices as an H.323 gatekeeper or one or more H.323 endpoints.

Voice Basics

To fully understand voice technology, both analog and digital transmission and signaling must be understood. Human speech and everything we hear is in analog form. Until several decades ago, the telephony network was based upon an analog infrastructure as well. The components of an early-generation analog phone call were a carbon microphone, a battery, an electromagnet, and an iron diaphragm. Connecting these components produced a method of transporting voice.

Although analog communication is ideal for human communication, analog transmission is neither robust nor efficient at recovering from line noise. In the early telephony network, when analog transmission was passed through amplifiers to boost the signal, not only did the voice get boosted, but the line noise was also amplified. This line noise resulted in an often-unusable connection.

Digital samples comprise one and zero bits. It is much easier for digital samples to be separated from line noise. Therefore, when signals are regenerated, a clean sound can be maintained. When the benefits of this digital representation became evident, the telephony network migrated to pulse code modulation (PCM).

PCM converts analog sound into digital form by sampling the analog sound 8000 times per second and converting each sample into a numeric code. The Nyquist theorem states that if you sample an analog signal at twice the rate of the highest frequency of interest, you can accurately reconstruct that signal back into its analog form. Because most speech content is below 4000 Hz (4 kHz), the sampling rate needed is 8000 times per second (125 microseconds between samples).

After the waveform is sampled, it is converted into a discrete digital form. This sample is represented by a code that indicates the amplitude of the waveform at the instant the sample was taken. The telephony form of PCM uses 8 bits for the code and a logarithm compression method that assigns more bits to lower-amplitude signals. The transmission rate is obtained by multiplying 8000 samples per second times 8 bits per sample, giving 64,000 bits per second, the standard transmission rate for one channel of telephone digital communications.

Two basic variations of 64-kbps PCM are commonly used: mu-law and a-law. The methods are similar in that they both use logarithmic compression to achieve 12 to 13 bits of linear PCM quality in 8 bits, but are different in relatively minor compression details (mu-law has a slight advantage in low-level signal-to-noise ratio performance). Usage has historically been along country and regional boundaries, with North America using mu-law and Europe using a-law modulation.

Another compression method often used is adaptive differential pulse code modulation (ADPCM). A commonly used instance of ADPCM, ITU-T G.726 encodes using 4-bit samples, giving a transmission rate of 32 kbps. Unlike PCM, the 4 bits do not directly encode the amplitude of speech, but the differences in amplitude as well as the rate of change of that amplitude, employing some very rudimentary linear prediction.

PCM and ADPCM are examples of “waveform” coders-decoders (codecs)—compression techniques that exploit redundant characteristics of the waveform itself. New compression techniques have been developed over the past 10 to 15 years that further exploit knowledge of the source characteristics of speech generation. These techniques employ signal-processing techniques that compress speech by sending only simplified parametric information about the original speech excitation and vocal tract shaping, requiring less bandwidth to transmit that information. These techniques can be grouped together generally as “source” codecs, and include variations such as linear predictive coding (LPC), code-excited linear prediction (CELP), and multipulse, multilevel quantization (MP-MLQ).

CELP, MP-MLQPCM, and ADPCM coding schemes are standardized by the ITU-T in its G-series recommendations. The most popular voice-coding standards for telephony and packet voice include:

- *G.711, which describes the 64-kbps PCM voice-coding technique outlined earlier*—G.711-encoded voice is already in the correct format for digital voice delivery in the public phone network or through private branch exchanges (PBXs).
- *G.726, which describes ADPCM coding at 40, 32, 24, and 16 kbps*—ADPCM voice may also be interchanged between packet voice and public phone or PBX networks, provided that the latter has ADPCM capability.
- *G.728, which describes a 16-kbps low-delay variation of CELP voice compression*—CELP voice coding must be transcoded to a public telephony format for delivery to or through telephone networks.
- *G.729, which describes CELP compression that enables voice to be coded into 8-kbps streams*—Two variations of this standard (G.729 and G.729 Annex A) differ largely in computational complexity, and both generally provide speech quality as good as that of 32-kbps ADPCM.
- *G.723.1, which describes a compression technique that can be used for compressing speech or other audio signal components of multimedia service at a very low bit rate, as part of the overall H.324 family of standards*—This coder has two bit rates associated with it—5.3 and 6.3 kbps; the higher bit rate is based on MP-MLQ technology and has greater quality; the lower bit rate is based on CELP, gives good quality, and provides system designers with additional flexibility.

As codecs rely more and more on subjectively tuned compression techniques, standard objective quality measures such as total harmonic distortion and signal-to-noise ratios have less correlation with perceived codec quality. A common benchmark for quantifying the performance of the speech codec is the mean opinion score (MOS). Because voice quality and sound in general are subjective to the listener, it is important to get a wide range of listeners and sample material. MOS tests are given to a group of listeners who give each sample of speech material a rating of 1 (poor) to 5 (excellent). The scores are then averaged to get the MOS. MOS testing is also used to compare how well a particular codec works under varying circumstances, including differing background noise levels, multiple encodes and decodes, different languages, and so on. This data can then be used to compare against other codecs.

Attacks Against the IP Telephony Network

Packet Sniffers/Call Interception

A packet sniffer is a software application that uses a network adapter card in promiscuous mode (a mode in which the network adapter card sends all packets received on the physical network wire to an application for processing) to capture all network packets that are sent across a particular collision domain. Sniffers are used legitimately in networks today to aid in troubleshooting and traffic analysis. However, since voice transport mechanisms generally don’t use encryption, the voice steams can saved and reassembled for listening. The tool “voice over misconfigured Internet telephones” (also known as vomit), takes an IP phone conversation trace captured by the UNIX tool tcpdump, and reassembles it into a wave file for easy listening. The phones are not actually misconfigured. Rather, if someone was able to obtain access to the IP data stream at any point in the network they could eavesdrop.

Virus and Trojan-Horse Applications

The primary vulnerabilities for end-user workstations are viruses and Trojan horse attacks. Viruses refer to malicious software that is attached to another program to execute a particular unwanted function on a user's workstation. An example of a virus is a program that is attached to command.com (the primary interpreter for windows systems), which deletes certain files and infects any other versions of command.com that it can find. A Trojan horse is different only in that the entire application was written to look like something else, when in fact it is an attack tool. An example of a Trojan horse is a software application that runs a simple game on the user's workstation. While the user is occupied with the game, the Trojan horse mails a copy of itself to every user in the user's address book. Then other users get the game and play it, thus spreading the Trojan horse.

We should be concerned about viruses and Trojan-horses in the data segment because they infect the PC-based IP Phone hosts that connect to the voice segment.

Unauthorized Access

Although unauthorized-access attacks are not a specific type of attack, they refer to most attacks executed in networks today. In order for someone to brute-force attack a Telnet login, he/she must first get the Telnet prompt on a system. Upon connection to the Telnet port, a message might indicate: “authorization required to use this resource.” If the hacker continues to attempt access, his/her actions become “unauthorized.” These kinds of attacks can be initiated on both the outside and inside of a network. Hackers may attempt to gain unauthorized access to the voice services with malicious intent in mind.

Caller Identity Spoofing

This type of attack occurs when a hacker is able to trick a remote user into believing they are talking to someone when in fact they are really talking to the hacker. This type of attack typically occurs with the hacker assuming the identity of someone who is not familiar to the target. A complex attack would be to first place a rogue IP phone in the network and then via a secondary exploit assume the identity of a valid IP phone (assuming the identity that you want your target to see). On the other hand it may be as simple as a bypassing physical building security and using an unattended IP phone!

Toll Fraud

This attack constitutes theft of service, namely phone calls. There are numerous methods the hacker could use to accomplish this task. In its basic case toll fraud includes an unauthorized user accessing an unattended IP phone to place calls. A more complex attack might include placing a rogue IP phone or gateway on the netwrk to place unaothrized calls.

Repudiation

If two parties talk over the phone and later on one party denies that the fact that the conversation ever happened, what proof would the other party have that it ever occurred? This type of attack is not all that common and is difficult to mitigate. Call logging is available however without strong user authentication (and users who logout when not using their IP phones) it is not possible to validate who actually placed the call rather only from which IP phone.

IP Spoofing

An IP spoofing attack occurs when a hacker inside or outside a network impersonates the conversations of a trusted computer. A hacker can do this in one of two ways. The hacker uses either an IP address that is within the range of trusted IP addresses for a network or an authorized external IP address that is trusted and to which access is provided to specified resources on a network. IP spoofing attacks are often a launch point for other attacks. The classic example is to launch a denial-of-service (DoS) attack using spoofed source addresses to hide the hacker's identity. As it relates to IP telephony, without spoof mitigation filters a hacker might be able to spoof the address of the call-processing manager and UDP flood the entire voice segment.

Denial of Service

Certainly the most publicized form of attack, denial of service (DoS) attacks are also among the most difficult to completely eliminate. Even among the hacker community, DoS attacks are regarded as trivial and considered bad form because they require so little effort to execute. Still, because of their ease of implementation and potentially significant damage, DoS attacks deserve special attention from security administrators. If you are interested in learning more about DoS attacks, researching the methods employed by some of the better known attacks can be useful.

These attacks include the following:

- TCP SYN Flood
- Ping of Death
- UDP fragment flood
- ICMP fragment flood

If not properly mitigated, all of these sample DoS attacks could render a voice segment unusable.

Application Layer Attacks

Application layer attacks can be implemented using several different methods. One of the most common methods is exploiting well-known weaknesses in software that are commonly found on servers, such as sendmail, HTTP, and FTP. By exploiting these weaknesses, hackers can gain access to a computer with the permissions of the account running the application, which is usually a privileged system-level account. These application layer attacks are often widely publicized in an effort to allow administrators to rectify the problem with a patch. Unfortunately, many hackers also subscribe to these same mailing lists, resulting in their learning about the attack at the same time (if they haven't discovered it already).

The primary problem with application layer attacks is that they often use ports that are allowed through a firewall. For example, a hacker executing a known vulnerability against a Web server often uses TCP port 80 in the attack. Because the Web server serves pages to users, a firewall needs to allow access on that port. From the perspective of the firewall, it is merely standard port 80 traffic. For this reason HIDS is also used on call-process managers even though they are protected by a stateful firewall. This is the most common method of gaining access to devices.

Trust Exploitation

Although not an attack in and of itself, trust exploitation refers to an attack where an individual takes advantage of a trust relationship within a network. The classic example is a perimeter network connection from a corporation. These segments often house DNS, Simple Message Transfer Protocol (SMTP), and HTTP servers. Because they all reside on the same segment, a compromise of one system can lead to the compromise of other systems because they might trust other systems attached to their same network. Another example is a system on the outside of a firewall that has a trust relationship with a system on the inside of a firewall. When the outside system is compromised, it can take advantage of that trust relationship to attack the inside network. This type of attack rarely surfaces in a secure IP telephony design. However, if multiple voice and data servers reside in the same segment, and the data server is compromised, it may then be possible to compromise the voice server as well even though they are both protected by a stateful firewall.

Appendix C: Architecture Taxonomy

Firewall: Stateful packet-filtering device that maintains state tables for IP-based protocols. Traffic is allowed to cross the firewall only if it conforms to the access-control filters defined, or if it is part of an already established session in the state table.

Router: A wide spectrum of flexible network devices, which provide many routing and security services for all performance requirements. Most devices are modular and have a range of LAN and WAN physical interfaces.

Host IDS: Host intrusion detection system is a software application that monitors activity on an individual host. Monitoring techniques can include validating operating system and application calls, checking log files, file system information, and network connections.

Network IDS: Network intrusion detection system. Typically used in a nondisruptive manner, this device captures traffic on a LAN segment and tries to match the real-time traffic against known attack signatures. Signatures range from atomic (single packet and direction) signatures to composite (multipacket) signatures requiring state tables and Layer 7 application tracking.

Application server: Provides application services directly or indirectly for enterprise end users. Services can include workflow, general office, and security applications.

Management server: Provides network management services for the operators of enterprise networks. Services can include general configuration management, monitoring of network security devices, and operation of the security functions.

Call-process manager: Provides call setup/establishment and customizable user-based configurations; also known as "IP PBX."

Voice-mail system: Provides IP-based voice-mail storage and autoattendant.

PC-based IP Phone: Any application that has the ability to reside on a user system (for example, desktop) and place calls to other IP telephony systems over the IP network.

Voice-enabled router: A router as defined previously with the additional capabilities of call processing (as listed previously) and legacy voice systems support (for example, Public Switched Telephone Network [PSTN]).

References

RFCs and Drafts

For a listing of the H.323 standard and associated components, refer to the primer and www.itu.int.

RFC 2543—*SIP: Session Initiation Protocol*:
http://www.cisco.com/warp/public/788/voip/voice_rfcs.html

RFC 2705—*MGCP: Media Gateway Control Protocol*
http://www.ietf.org/rfc/rfc2705.txt?number=2705

For all other voice-related RFCs:
http://www.cisco.com/warp/public/788/voip/voice_rfcs.html

Miscellaneous References

Securing Cisco Unity Server:
http://cco/univercd/cc/td/doc/product/voice/c_unity/whitpapr/security.htm

Securing Cisco CallManager:
http://www.cisco.com/warp/public/788/AVVID/ids_host_sensor_cm.html

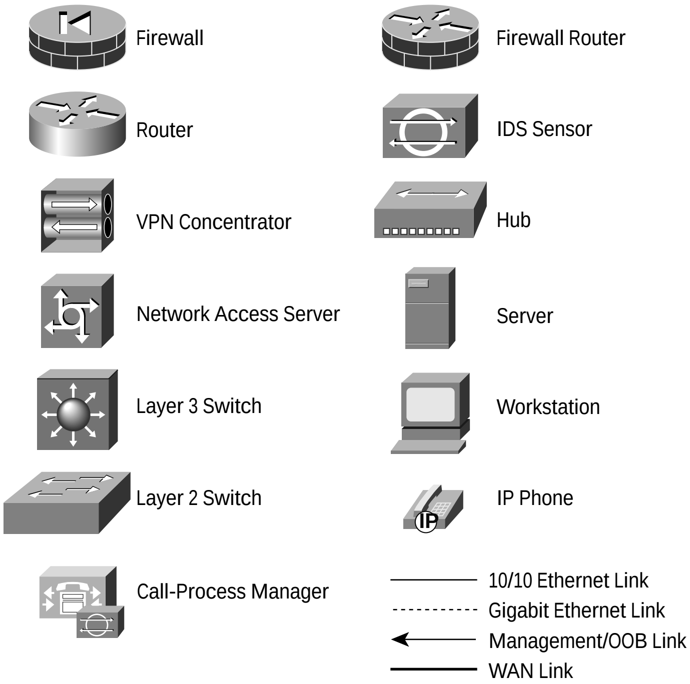
General Telephony Network Guidelines:
http://www.cisco.com/univercd/cc/td/doc/product/voice/ip_tele/solution/6_operat.htm
http://vomit.xtdnet.nl/

Arpwatch:
http://www-nrg.ee.lbl.gov/nrg.html

Partner Product References

General Cisco AVVID Security and VPN Solution Partners Information: http://www.cisco.com/go/securitypartners

Figure C-1
Diagram Legend



Acknowledgments

The authors would like to publicly thank all the individuals who contributed to the SAFE architecture and the writing of this document. We give special thanks to Earl Carter, Todd Truitt, and Diane Andrada for their efforts. Certainly, the successful completion of this architecture would not have been possible without the valuable input and review feedback from all of the Cisco employees both in corporate headquarters and in the field. In addition, many individuals contributed to the lab implementation and validation of the architecture. Thank you all for your special effort.

CISCO SYSTEMS

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems Europe
11, Rue Camille Desmoulins
92782 Issy-les-Moulineaux
Cedex 9
France
www-europe.cisco.com
Tel: 33 1 58 04 60 00
Fax: 33 1 58 04 61 00

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 317 7777
Fax: +65 317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the

Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

LW2987 02/02