- Examining SAFE IP Telephony Design Fundamentals
- Understanding SAFE IP Telephony Axioms
- Understanding SAFE IP Telephony Network Designs

CHAPTER 19

SAFE IP Telephony Design

This chapter introduces the SAFE network design for IP telephony, which Cisco Systems developed to address customer concerns with the security of IP telephony deployed in a network. The “SAFE: IP Telephony Security in Depth” whitepaper examines the security of IP telephony in each of the SAFE blueprints—enterprise, medium-sized, and small networks—and builds on the concepts of modularity and “defense in depth.” The whitepaper also addresses the unique security issues that an IP telephony deployment poses to a network.

“Do I Know This Already?“ Quiz

The purpose of the “Do I Know This Already?” quiz is to help you decide if you really need to read the entire chapter. If you already intend to read the entire chapter, you do not necessarily need to answer these questions now.

The 13-question quiz, derived from the major sections in “Foundation Topics” portion of the chapter, helps you determine how to spend your limited study time.

Table 19-1 outlines the major topics discussed in this chapter and the “Do I Know This Already?” quiz questions that correspond to those topics.

Table 19-1 *“Do I Know This Already?” Foundation Topics Section-to-Question Mapping*

Foundations Topics Section	Questions Covered in This Section
Examining SAFE IP Telephony Design Fundamentals	1–2
Understanding SAFE IP Telephony Axioms	3–9
Understanding SAFE IP Telephony Network Designs	10–12

CAUTION The goal of self-assessment is to gauge your mastery of the topics in this chapter. If you do not know the answer to a question or are only partially sure of the answer, you should mark this question wrong for purposes of the self-assessment. Giving yourself credit for an answer you correctly guess skews your self-assessment results and might provide you with a false sense of security.

1. Which of the following objectives are fundamental in the design of SAFE IP telephony networks?
   a. Designation of responsibility
   b. Quality of service
   c. Integration with existing network infrastructure
   d. Authentication of users and devices (identity)
   e. Flexibility of the design
   f. Secure management
2. What network feature should be deployed throughout the network infrastructure to ensure a successful IP telephony design?
   a. QoS
   b. ACLs
   c. Authentication
   d. IDS
   e. IPS
3. Which of the following is one of the key axioms in the SAFE IP telephony design?
   a. Security and attack mitigation based on policy
   b. Voice and data segmentation
   c. User authentication
   d. Options for high availability (some designs)
   e. Secure management
4. Which of the following protocols currently are used in IP telephony products?
   a. IGMP
   b. MGCP
   c. SIP
   d. CGMP
   e. CDP
   f. Q.773
   g. H.323
5. Why does a firewall need to be "intelligent" when dealing with H.323 traffic?
   a. The firewall must be capable of recognizing the traffic to encrypt it properly.
   b. H.323 uses multiple static ports for signaling and media streams, and the firewall needs to know about those.

c. H.323 traffic must be authenticated at the firewall, and, therefore, the firewall needs to be capable of recognizing that traffic.

d. H.323 utilizes multiple dynamic ports for call sessions, and the firewall must be capable of determining those ports from the signaling channel.

e. H.323 cannot use NAT, and, therefore, the firewall must be capable of identifying H.323 traffic appropriately.

6. Which of the following is a tool that you can use to reconstruct a voice conversation?

    a. dsniff
    b. TCPdump
    c. ARPwatch
    d. VOMIT
    e. MITM

7. Which of the following are legitimate connections that should be allowed through the stateful firewall protecting the call-processing manager?

    a. PC web browser connecting to voice-mail server
    b. IP phone connecting to PC clients in the data segment
    c. Call establishment and configuration traffic
    d. Browsing of the IP phone web servers by PC clients
    e. Connections from IP phones in the voice segment and the voice-mail system
    f. Communication between the voice-mail system and the call-processing manager

8. What are the two most common recommended methods of authentication for IP phones?

    a. Device authentication
    b. Network authentication
    c. Proxy authentication
    d. User authentication
    e. Null authentication

9. Security design reliance should be based on which of the following?

    a. VLAN segmentation
    b. Data sharing between voice and data VLANs
    c. Access control
    d. Layered security best practices
    e. Multicast join restriction

10. Which of the following are services provided by the edge router in the small IP telephony design?
    a. VLAN segmentation
    b. Stateful firewalling
    c. NAT
    d. QoS
    e. All of these answers are correct
11. What is the purpose of the call-processing manager in each of the SAFE IP telephony designs?
    a. The call-processing manager provides data services to IP telephony devices in the module.
    b. The call-processing manager provides voice services to IP telephony devices in the module.
    c. The call-processing manager does not provide voice-mail storage in the modules.
    d. The call-processing manager provides data storage for the IP phones.
12. What two basic designs are possible in the small and medium blueprints for IP telephony?
    a. Hub
    b. Spoke
    c. Headend
    d. Remote
    e. Branch
13. What is the purpose of the Layer 3 switches in the server module?
    a. The switches in the module are not Layer 3 switches; they are Layer 2 switches.
    b. No special purpose is assigned to the Layer 3 switches in this module.
    c. The Layer 3 switches provide routing and switching services to both voice and data traffic, in addition to filtering, QoS, VLANs, and private VLANs to the servers. They also provide for traffic inspection through the use of integrated NIDS.
    d. The Layer 3 switches provide firewall services through the use of an integrated firewall service module.

The answers to the "Do I Know This Already?" quiz are found in Appendix A, "Answers to the 'Do I Know This Already?' Quizzes and Q&A Sections." The suggested choices for your next step are as follows:

- **11 or less overall score**—Read the entire chapter. This includes the "Foundation Topics" and "Foundation Summary" sections and the Q&A section.
- **12 or 13 overall score**—If you want more review on these topics, skip to the "Foundation Summary" section and then go to the Q&A section. Otherwise, move to the next chapter.

Foundation Topics

Examining SAFE IP Telephony Design Fundamentals

The "SAFE: IP Telephony Security in Depth" whitepaper provides best-practice information for the deployment of IP telephony in the various SAFE blueprints. Although this whitepaper covers a wide range of topics related to IP telephony, it does not discuss many other topics, including quality of service (QoS) applied to the voice traffic to eliminate echoes and jitter, and the security of the voice protocols between the voice gateways. Because of the nature of IP telephony and the requirements for low latency, QoS is an extremely important feature that you must enable network-wide before deploying IP telephony. The whitepaper focuses on centralized call processing, not distributed call processing. It is assumed, however, that all remote sites have a redundant link to the headend or the local call-processing backup, in case of headend failure. Finally, the interaction between IP telephony and Network Address Translation (NAT) is not covered.

The following design objectives guided the decision-making process for the SAFE IP telephony whitepaper:

- 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

The SAFE IP telephony design must provide telephony services in the same way that current telephony services are deployed. In addition, it must maintain the same characteristics as traditional telephony in as secure a manner as possible. Finally, it must integrate with existing network designs.

IP Telephony Network Components

IP telephony adds four voice-specific devices to a network:

- **IP telephony devices**—This category includes any device that supports placing calls in an IP telephony network, such as IP phones and PC softphones (IP phone software running on a PC).

- **Call-processing manager**—This system is the server that provides call control and configuration management for IP telephony devices in the network. It provides bootstrap information for IP telephony devices, call setup, and call routing throughout the network to other voice-enabled devices such as voice gateways and voice-mail systems.
- **Voice-mail system**—This system primarily provides IP-based voice-mail storage services. In addition, it can provide user directory lookup capabilities and call-forwarding features.
- **Voice gateway**—This is a generic term that refers to any gateway that provides voice services, such as IP packet routing, backup call processing, Public Switched Telephone Network (PSTN) access, and other voice services. This device is the interface between the legacy voice systems that can provide backup for the IP telephony network in case of failure. This device is typically not a full-featured call-processing manager; it supports a subset of the call-processing functionality provided by the call-processing manager.

VoIP Protocols

At the time of writing of the "SAFE: IP Telephony Security in Depth" whitepaper, these were the three predominant protocol standards for voice over IP (VoIP):

- H.323
- Session Initiation Protocol (SIP)
- Media Gateway Control Protocol (MGCP)

The following sections describe each standard in detail.

H.323

The International Telecommunication Union (ITU) H.323 standard covers IP devices that participate in and control H.323 sessions, along with elements that interact with switched-circuit networks. This standard does not cover the LAN itself or the transport layer within the network. H.323 provides for point-to-point or multipoint sessions. The H.323 standard is composed of several components, including other standards that describe call control, signaling, registration, and packetization/synchronization of media streams. Table 19-2 lists these components.

Table 19-2 *Core Components of H.323*

Component	Function
H.225	Specifies messages for call control, signaling, registration, admission, packetization, and synchronization
H.245	Specifies the requirements for opening and closing channels for media streams and other commands

Table 19-2 *Core Components of H.323 (Continued)*

Component	Function
H.261	Video codec for audiovisual services
H.263	Specification for a new video codec for basic video 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.723	Audio codec—5.3 kbps and 6.3 kbps modes
G.728	Audio codec—3.1 kHz at 16 kbps
G.729	Audio codec—3.1 kHz at 8 kbps

Ports used for H.245 signaling and media channels dynamically are negotiated between the endpoints. This makes it especially difficult to impose security policy and traffic shaping. Additionally, the control channel of H.245 uses TCP as a transport protocol, but the media stream channels utilize UDP as a transport protocol. For a firewall to be placed between two (or more) H.323 endpoints, the firewall must be either H.323 enabled (that is, it must be intelligent enough to allow H.323 traffic through, appropriately utilizing an H.323 proxy) or it must monitor the control channel to determine which dynamic ports are in use for the H.323 sessions.

SIP

The Session Initiation Protocol (SIP) is an ASCII-encoded application layer control protocol that is defined in RFC 2543. You can use SIP to establish, maintain, and terminate calls between two or more endpoints. Like other protocols, it is designed to address the signaling and session-management functions in an IP telephony network. SIP does this by allowing call information to be carried across network boundaries and also by providing the capability to control calls between any endpoints.

SIP can identify the location of an endpoint through the use of address resolution, name mapping, and call redirection. Additionally, through the use of the Session Description Protocol (SDP), the protocol can determine the least common denominator of possible services between the two endpoints. This provides the capability to establish conference calls using only the media capabilities that all participants can support. SIP also can handle the transfer and termination of calls and the determination of the availability of a given endpoint, and can establish a session between two or more endpoints (as in a conference).

MGCP

The Media Gateway Control Protocol (MGCP) is a master/slave protocol implemented in media gateway controllers or call agents. These controllers/agents run on telephony gateways, which are devices that provide the conversion of data packets used in IP telephony to audio signals that are carried on PSTN circuits. The controllers/agents provide the control, signaling, and processing skills to control the telephony gateways and implement the signaling layers of H.323. To other H.323 devices, these controllers/agents appear as an H.323 gatekeeper or as one or more H.323 endpoints.

Threats to IP Telephony Networks

Various threats are inherent in all networks but are of particular importance where IP telephony is deployed. This section describes the following threats:

- Packet sniffers/call interception
- Virus and Trojan horse applications
- Unauthorized access
- Caller identity spoofing
- Toll fraud
- Repudiation
- IP spoofing
- Denial of service
- Application layer attacks
- Trust exploitation

Packet Sniffers/Call Interception

A packet sniffer can monitor and capture the traffic in a network. A packet sniffer in a voice VLAN can capture unencrypted conversations and save them to a file. These conversations can then be reassembled for listening using such tools as Voice over Misconfigured IP Telephony (VOMIT).

Virus and Trojan Horse Applications

Viruses are malicious software that attached to other files and programs and executed by either the user opening the file or program startup. Examples of viruses include the Melissa virus and the more recent MyDoom and W32.bagle viruses.

A Trojan horse application is a program designed to appear innocuous to the user while it executes additional commands without the user's direct knowledge. A simple example is a computer game that, while the user is playing it, deletes specific files from the machine or installs a back-door mechanism for an external attacker to gain access to the system. A Trojan horse application is of particular concern because if the targeted PC is on the data segment of a network with IP telephony deployed and a PC softphone installed (thereby requiring access to the voice VLAN), an attacker might be able to bypass the segmentation between the two VLANs by installing a Trojan horse application on that system.

Unauthorized Access

Although these are not specific types of attacks, they are the most common attacks executed in today's networks. Many modern IP phones also behave as a switch providing access to both the voice and the data VLAN. An attacker could plug into the back of an IP phone and gain instant access to the network, possibly without requiring authentication.

Caller Identity Spoofing

Caller identity spoofing is much like IP spoofing. The attacker's main goal is to trick a remote user into believing that he or she is communicating with someone other than the attacker. This attack typically requires that the hacker assume the identity of someone who is not familiar to the target and can be either complex enough to require the placement of a rogue IP phone on the network or as simple as using an unattended IP phone.

Toll Fraud

Toll fraud encompasses a wide variety of illegal behavior. Typically, this involves the theft of the phone service. In its most basic form, toll fraud involves an unauthorized user accessing an unattended IP telephone and placing calls. Other attacks include placing a rogue IP phone or gateway in the network to place unauthorized calls.

Repudiation

Repudiation attacks are difficult to mitigate. If two parties talk over the phone and one party decides later to deny that the conversation took place, the other party has no proof that the conversation ever took place. However, call logging can be used to verify that a communication did take place. Without strong user authentication, however, validating who placed the call is not possible.

IP Spoofing

IP spoofing involves the impersonation of a trusted system. To do this, an attacker uses either an IP address that is within the range of trusted IP addresses or a trusted external IP address that also is provided access to target resources on the network. IP spoofing typically is associated with certain types of attacks, such as a denial-of-service (DoS) attack, in which the attacker wants to hide his or her true identity.

Denial of Service

Denial-of-service (DoS) attacks are one of the most difficult attacks to mitigate completely. DoS attacks against the call-processing manager in an IP telephony deployment can bring down the entire phone system.

Application Layer Attacks

Application layer attacks are attacks against an application such as IIS, sendmail, or Oracle that are running on a system. Exploiting weaknesses in these applications can provide an attacker with access (sometimes privileged access) to the system. Because these attacks are against applications that have ports that often are allowed through a firewall, it is critical that these attacks be mitigated through other means. For IP telephony networks, the most important element is the call-processing manager. Because many call-processing managers run a web server for remote access to management functions, they can be attacked through that application. It is important that a host-based IPS be installed and active on call-processing managers even though they might be protected by a stateful firewall to prevent application layer attacks.

Trust Exploitation

A trust-exploitation attack as it relates to IP telephony can be executed if voice and data servers have a trust relationship. The exploitation of the data server, such as a web server, then could result in the exploitation of the central call-processing manager. This provides the attacker with significant access into not just the data VLAN, but also the voice VLAN.

Understanding SAFE IP Telephony Axioms

SAFE IP telephony assumes conformance to the original SAFE axioms, as discussed in the "SAFE: A Security Blueprint for Enterprise Networks" whitepaper (refer to Chapter 3, "SAFE Design Concepts"). In addition to these, the SAFE IP telephony work introduces other axioms to the design that are specific to IP telephony networks:

- Voice networks are targets.
- Data and voice segmentation is key.
- Telephony devices do not support confidentiality.
- IP phones provide access to the data-voice segments.
- PC-based IP phones require open access.
- PC-based IP phones are especially susceptible to attack.
- Controlling the voice-to-data segment interaction is key.

- Establishing identity is key.
- Rogue devices pose serious threats.
- Secure and monitor all voice servers and segments.

Each of these axioms is described in greater detail next.

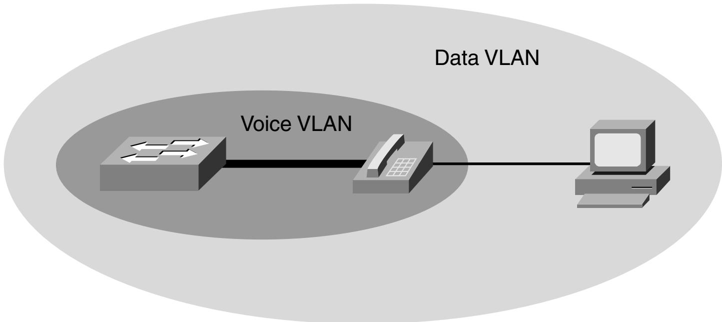
Voice Networks Are Targets

Voice networks increasingly represent high-value targets for attacks. Attacks can range from a practical joke on company employees through a company-wide voice-mail recording telling all employees to take a day off, to eavesdropping on the chief financial officer's conversations with analysts discussing the company's earnings before being announced, to eavesdropping on internal calls regarding customers. Voice networks today represent a greater risk to security than any other technology; it is imperative that these networks be secured as tightly as possible to reduce the impact that an attack can have on both the voice network and the data network.

Data and Voice Segmentation Is Key

Although IP-based telephony traffic can share the same physical network as data traffic, it should be segmented to a separate virtual LAN (VLAN) to provide additional QoS, scalability, manageability, and security, as shown in Figure 19-1. Segmenting telephony traffic from data traffic greatly enhances the security of the IP-based telephony traffic and allows for the same physical infrastructure to be leveraged.

Figure 19-1 *Data and Voice Segmentation*



Telephony Devices Do Not Support Confidentiality

IP-based telephony uses the same underlying physical infrastructure as the data network. As such, it is possible for an attacker to gain access to the telephony stream using a variety of attack tools. One of the most popular of these tools is called VOMIT. This tool reconstructs the data stream of the voice traffic captured using another tool, such as TCPdump or snoop; reconstructs the voice traffic; and outputs a WAV sound file. Although the phone is not actually *misconfigured*, this example reinforces the need to segment the voice and data traffic on the network. The use of a switched infrastructure is critical to that effort and becomes significantly advantageous in the capability to tune network intrusion detection systems (NIDS). However, even a switched infrastructure can be defeated by tools such as dsniff. dsniff can turn the switched medium into a shared medium, thus defeating the benefits of the switch technology. Another way that an attacker can defeat a switched medium is to plug a workstation into a network port in place of an IP phone.

IP Phones Provide Access to the Data-Voice Segments

IP phones typically provide a second network port so that a PC or workstation can plug into the phone, which then plugs into the network port. This provides the simplicity of a single cable for network connectivity. When this is the case, it is critical that you follow the data/voice segmentation principle. Some IP phones provide for simple Layer 2 connectivity, in which the phone acts as a hub; others provide switched infrastructure capabilities and can understand VLAN technology such as 802.1q tags. The phones that are VLAN capable support the segmentation of the data and voice segments through the use of 802.1q tags. However, your security design should not be based solely on VLAN segmentation; it should implement layered security best practices and Layer 3 access control in the distribution layer of the design.

PC-Based IP Phones Require Open Access

In addition to standalone IP phones, you have the option of PC-based IP phones. However, because these are software-only IP telephony devices, they reside on the data segment of the network but require access to the voice segment, thus violating the second axiom: *Data and voice segmentation is key.* As such, using PC-based IP phones is not recommended without the presence of a stateful firewall to broker the data-voice interaction. IP-based telephony devices typically use UDP port numbers greater than 16384. Without a stateful firewall in place to broker the connections between the data and voice segments, a wide range of UDP ports would have to be permitted through a filter. As a result, securing all connections between the two segments would be impossible. A stateful firewall is required to prevent an attack from one segment to the other.

PC-Based IP Phones Are Especially Susceptible to Attack

PC-based IP phones represent a significant difficulty in an IP telephony deployment. Unlike their standalone IP phone brethren, PC phones run on top of standard operating systems such as Microsoft Windows, which leaves them vulnerable to many of the same application, service, and OS attacks. Another difficulty is that PC-based IP phones reside in the data segment of the network and thus are susceptible to attacks such as Code-Red, Nimda, and SQL Slammer. In these examples, the worms bog down the PC-based IP phone user systems and the segments they reside in to such an extent that they are unusable.

Controlling the Voice-to-Data Segment Interaction Is Key

Controlling the voice-to-data segment interaction is critical to successfully deploying and securing an IP telephony system. The best way to accomplish this task is to use a stateful firewall. This type of firewall provides denial-of-service (DoS) protection against connection starvation and fragmentation attacks; allows dynamic, per-port access to the network; and provides spoof mitigation and general packet filtering. The placement of the stateful firewall is limited to areas of the network where the voice and data segments interact. These legitimate connections should be allowed:

- Communication between the voice-mail system and the call-processing manager if one is located in the data segment.
- Call establishment and configuration traffic between IP phones in a voice segment connecting to the call-processing manager in another voice segment.
- Connections from IP phones in the voice segment and the voice-mail system, if it is located in the data segment.
- IP phones in the voice segment browsing resources outside the voice segment through the proxy server. This requires that the proxy server be capable of accessing resources in the data segment or another voice segment through the firewall. Additionally, the firewall should broker users in the data segment browsing the call-processing manager in the voice segment.
- If PC-based IP phones are deployed, the firewall must broker connections from the PC-based IP phones in the data segment connecting to the call-processing manager in the voice segment. In addition, if the voice-mail system is in the voice segment, connections from the PC-based IP phones to this system must be brokered by the stateful firewall.

It is recommended that you use RFC 1918 address spaces for all IP telephony devices, to reduce the possibility of voice traffic traversing outside the network. The added benefit to using RFC 1918 addresses is that attackers will not be able to easily scan for vulnerabilities because NAT will be configured on the firewall. If possible, use different RFC 1918 addresses for both the voice and data segments.

Establishing Identity Is Key

Device authentication in an IP telephony deployment typically is based on the MAC address of the phone. The IP telephone tries to retrieve its network configuration from the call-processing manager using the MAC address as the identification string. If the call-processing manager has no knowledge of a specific MAC address being provided by an IP telephony device (whether it is an IP phone or PC-based IP phone), it will not provide the network configuration to the device.

When possible, it is recommended that you apply user authentication in addition to device authentication. With user authentication, the user must log into a phone with a password or PIN before telephony services are provided. This feature originally was designed for shared office spaces and enables you to provide a custom configuration based on user identity. Although a slight inconvenience factor is associated with user authentication, it helps to further mitigate the placement of rogue phones into the network and the placing of a call. The next section describes the threats associated with rogue devices in more detail.

Rogue Devices Pose Serious Threats

To mitigate the impact of rogue devices, it is recommended that you lock down the switch ports, network segments, and services in the network. Best practices, including disabling unused ports, discussed throughout the SAFE designs apply to IP telephony. In addition, the following four best practices provide mitigation details that are specific to IP telephony:

- Statically assign IP addresses to known MAC addresses in DHCP networks with IP phones deployed.
- Turn off the common temporary automatic phone registration feature that many call-processing managers have available. In addition, configure the call-processing managers to deny configuration information to unknown PC-based IP phones.
- Consider using a utility such as ARPwatch to monitor MAC addresses in the voice segment. ARPwatch is available at http://www-nrg.ee.lbl.gov/nrg.html.
- Filter in all network segments to restrict which devices can connect to the call-processing manager or the voice-mail system.

Secure and Monitor All Voice Servers and Segments

The same attacks that can cripple servers in the data segment can affect key voice servers in the voice segment. It is recommended that the same considerations given to production servers in the data segment be provided to the voice servers in the voice segment. These considerations include the following:

- Turn off all unneeded services.
- Update the operating system with the latest security patches.
- Harden the OS configuration.
- Disable unnecessary or unused features in the voice system.
- Do not run unnecessary applications on the voice servers.

In addition, deploy NIDS in front of the call-processing managers, to detect attacks sourced from the data segment, and host-based IPS on the call-processing managers themselves. NIDS also can be deployed between the voice and data segments, to detect any DoS attacks targeted against the voice segment specifically. Finally, it is recommended that the management axioms discussed in Chapter 3 be used when managing the voice servers.

Understanding SAFE IP Telephony Network Designs

The next sections discuss the deployment considerations for IP telephony in each of the SAFE network blueprints: the small, medium-sized, and enterprise networks. In each of these blueprints, adding IP telephony into the network infrastructure required some modification of devices that provide an interface between modules in the blueprint. Not all modules were affected by the incorporation of IP telephony into the network infrastructure; therefore, those modules were omitted from the discussion.

Branch Versus Headend Considerations

You can use the designs in small and medium-sized network configurations in one of two ways. In the first configuration, the design is acting as a branch of a larger enterprise. In the second configuration, the larger network design is considered the headend of the organization's network, and the smaller network designs can be considered the branch or satellite offices.

IP Telephony Deployment Models

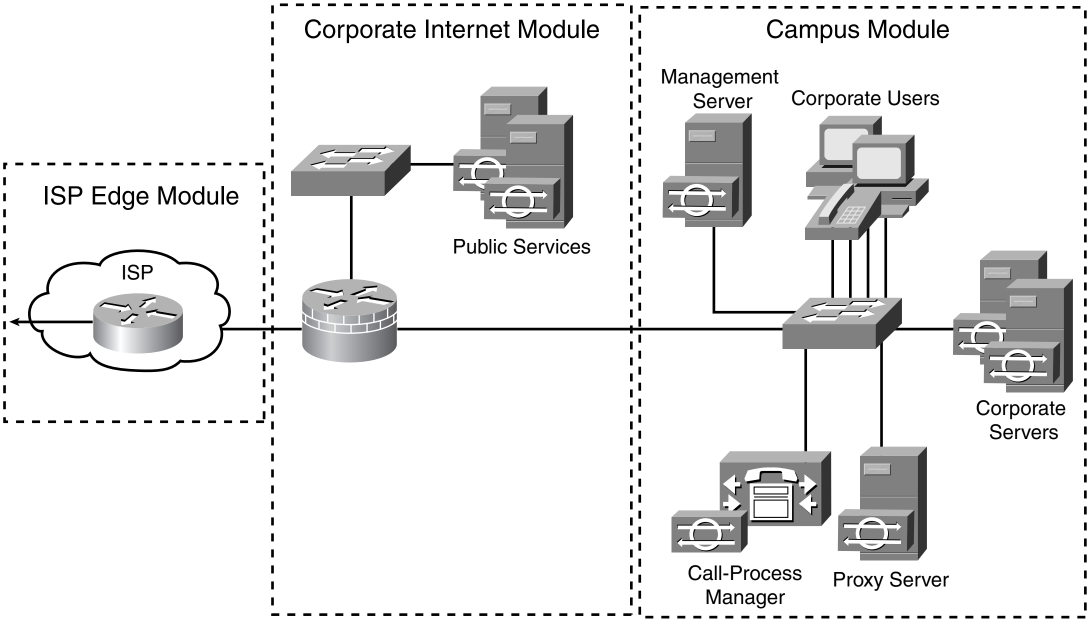
Three general models primarily exist for the deployment of IP telephony services throughout a network. The following deployment models are influenced by both the size and the distribution of the network (multiple branches, private networks, and so on):

- **Single-site campus**—This model is the most basic deployment model. All the IP telephony devices reside in a single, physically contiguous campus
- **WAN centralized call-processing**—In this model, multiple sites deploy IP telephony. These sites might be connected to a central campus over a private WAN or through the use of VPNs. The headend site, or campus, contains the only call-processing manager cluster; however, remote sites can have local voice services, such as voice mail.
- **WAN distributed call-processing**—This is the most complex design of the three models. In this model, multiple sites are connected through either a private WAN or over a VPN, and one or more of the sites contains a call-processing manager cluster. Many, although not all, of the sites have local voice services, such as voice mail. Some of the sites rely on others for their voice-mail services.

Small IP Telephony Network Design

The small IP telephony network design is based on the SAFE small network blueprint. This design is shown in Figure 19-2 and includes several minor modifications to the small blueprint design.

Figure 19-2 *Small IP Telephony Network Design*



As shown in Figure 19-2, the small IP telephony network design consists of the Corporate Internet module, the Campus module, and the ISP Edge module. The SAFE IP telephony modifications made to this blueprint focus only on the Corporate Internet and Campus modules. No modifications were made to the ISP Edge module because the service provider is not providing IP telephony services to the network.

Corporate Internet Module

The Corporate Internet module provides connectivity to the Internet for the small SAFE blueprint. The key device here is the voice-enabled edge firewall/router, which provides protection of network resources, stateful filtering, and voice services. The firewall/router mitigates toll fraud by limiting only known telephony devices from communicating with one another, as well as other attacks such as unauthorized access, DoS attacks, and IP spoofing attacks.

The voice-enabled firewall/router provides not just the typical security services, such as NAT, VPN, stateful firewall inspection of traffic, and IDS, but also voice services, including VLAN segmentation. In one VLAN reside the call-processing manager, the proxy server, and the IP phones. The user, management, and voice-mail/e-mail systems reside in the other VLAN.

Campus Module

The Campus module contains the end-user systems and the corporate servers, such as voice-mail servers, e-mail servers, management servers, IP phones, and the Layer 2 infrastructure. VLANs are enabled on the Layer 2 switch to provide segmentation between the voice and data traffic. Host IDS (HIDS) is deployed across all critical servers. The role of HIDS is more important in this design because of the lack of a Layer 3 router within the Campus module to provide access control between the VLANs.

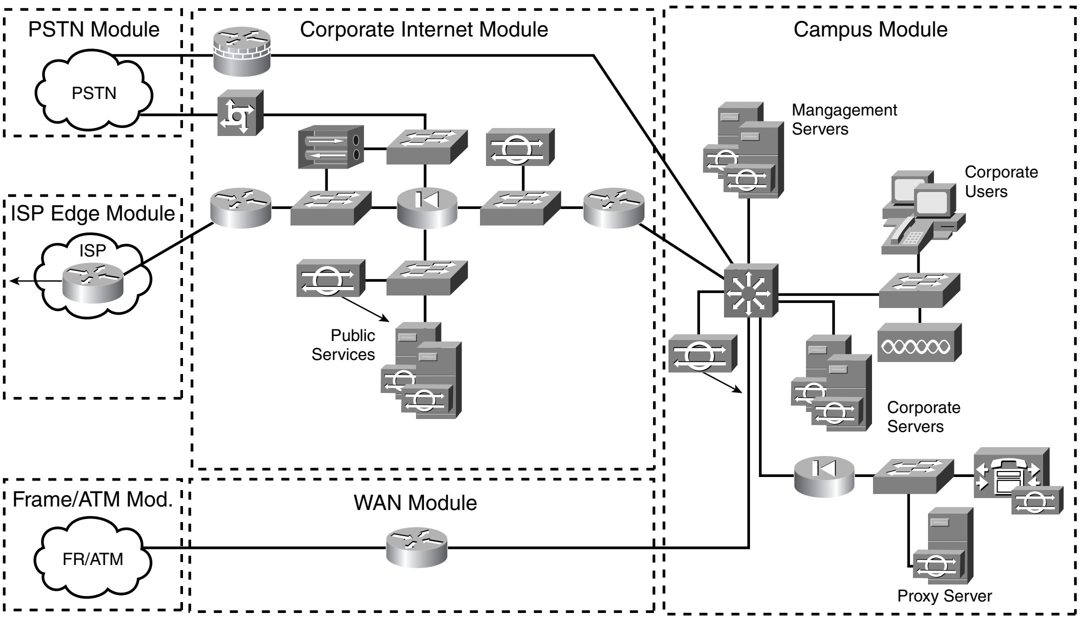
Design Alternatives for the Small IP Telephony Network

One alternative design is to provide two completely separate VLANs, with a Layer 3 access device providing traffic filtering between the VLANs. Another alternative is to place the voice-mail/e-mail server in the voice segment; however, this design is not recommended because the voice-mail/e-mail server is running additional services that are required in the data segment.

Medium-Sized IP Telephony Network Design

The medium-sized IP telephony network design shown in Figure 19-3 is based on the SAFE medium-sized network blueprint. No changes have been made except to the Campus module to support IP phones, PC-based IP phones, voice services, proxy services, PSTN for WAN backup and local calls, and VLANs for voice and data segmentation.

Figure 19-3 *Medium-Sized IP Telephony Network Design*



The Campus module and possible design alternatives are described in the next sections.

Campus Module

The key IP telephony devices in the campus module are provided in Table 19-3.

Table 19-3 *Key Devices in Campus Module*

Key Device	Functions
Layer 3 switch	Routes and switches voice and data traffic within the module.
Layer 2 switch (with VLAN support)	Provides network connectivity to endpoint user workstations and IP phones.
Corporate servers	Provide e-mail and voice-mail services to internal users, and file, print, and DNS resolution to workstations.
User workstation	Provides data services and voice services (through PC-based IP phones) to end users.
NIDS appliance	Provides Layer 4 to Layer 7 packet inspection.
IP phones	Provides voice services to end users.
Call-processing manager	Provides voice services to IP telephony devices in the module.
Proxy server	Provides data services to IP phones.
Stateful firewall	Provides network-level filtering for the call-processing manager and the proxy server.

The primary function of the Campus module is to switch data, voice, and management traffic while enforcing the network and voice VLAN separation. The VLAN separation is augmented by the use of filtering on the Layer 3 switch and also a stateful firewall. HIDS are used to protect both key voice services and the PC-based IP phone hosts. The stateful firewall and the Layer 3 switch control the traffic flows between the data and voice VLANs. The proxy server provides data services to IP phones; it also is located on the same VLAN as the call-processing manager. Private VLANs are used to mitigate local trust-exploitation attacks between the proxy server and the call-processing manager. For secure management, Layer 3 and Layer 4 filtering limits administration of key systems to authorized administration hosts. In addition, application-level security provides user authentication and confidentiality.

Performance is not a limitation in this design because all devices are situated on a Fast Ethernet network. The only limitation to this design is the number of IP telephony devices that the call-processing manager can support. If the number of IP telephony devices exceeds the capacity of the call-processing manager, additional call-processing managers are required.

Design Alternatives for the Medium-Sized IP Telephony Network

One possible alternative is to redesign the IP telephony network to take advantage of high-availability capabilities. This redesign would require the addition of another call-processing manager and another firewall in the Campus module, to provide resiliency. Another possibility is to move the voice-mail system off an additional demilitarized zone (DMZ) segment on the stateful firewall.

Large IP Telephony Network Design

The large IP telephony network design is based on the SAFE Enterprise network blueprint. This design already took IP telephony requirements into account. However, certain changes were made to this design in the "SAFE: IP Telephony Security in Depth" whitepaper. These changes include the following additions:

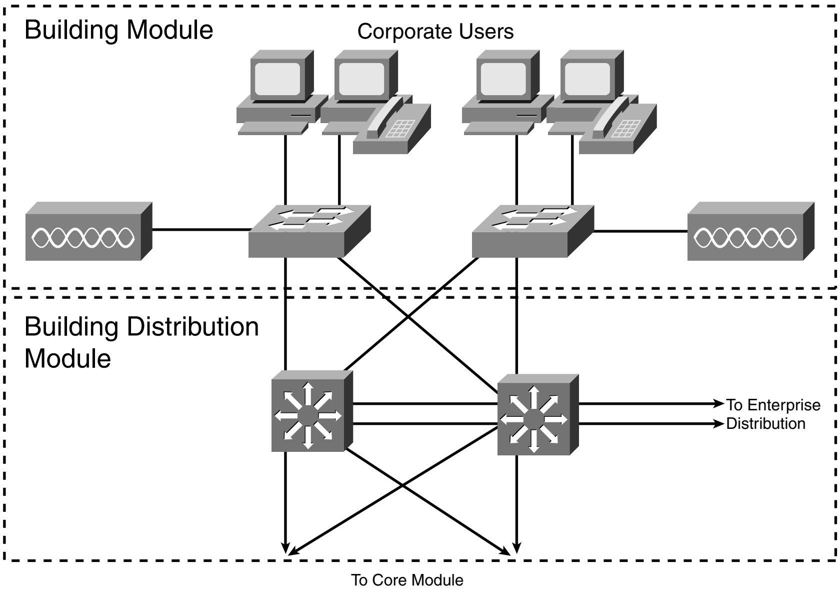
- PC-based IP phones
- Voice segment for the voice-mail system
- PSTN for local calls at the Edge Distribution module
- HIDS on all voice-related servers
- Call-processing manager and stateful firewall to provide resiliency in the design

This section focuses on the Building and Server modules, where the preceding changes were made.

Building Module

The Building and Building Distribution modules of the SAFE enterprise design are shown in Figure 19-4. The Building module provides switching functions for data and voice traffic, while at the same time enforcing segmentation between the two. This is done through stateless Layer 3 filtering and VLANs.

Figure 19-4 *Large IP Telephony Building and Building Distribution Modules*



The key devices in the Building module are listed in Table 19-4.

Table 19-4 *Key Devices in Large IP Telephony Building Module*

Key Device	Functions
Layer 2 switch (with VLAN support)	Provides network connectivity to endpoint user workstations and IP phones.
User workstation	Provides data services and voice services (through PC-based IP phones) to end users.
IP phones	Provide voice services to end users.

Server Module

The primary function of the Server module, shown in Figure 19-5, is to provide voice and data services throughout the design to end users and devices.

The Server module contains all the voice services needed for IP telephony in this design. The key devices in this module are provided in Table 19-5.

Figure 19-5 *Large IP Telephony Network Design*

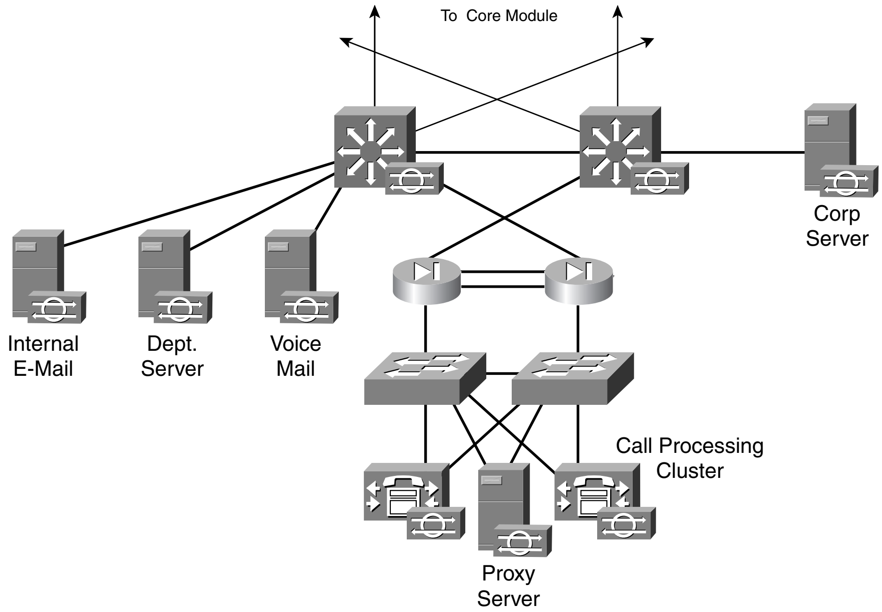


Table 19-5 *Key Devices in Server Module*

Key Device	Functions
Layer 3 switch	Routes and switches voice and data traffic within the module.
Corporate servers	Provide e-mail and voice-mail services to internal users, and provide file, print, and DNS resolution to workstations.
Call-processing manager	Provides voice services to IP telephony devices in the module.
Proxy server	Provides data services to IP phones.
Stateful firewall	Provides network-level filtering for the call-processing manager and the proxy server.

Although the call-processing manager, the proxy server, the voice-mail system, and the e-mail systems each reside in the same module, they are separated through VLAN segmentation. In addition, internally to the VLANs, servers can be separated further through the use of private VLANs to mitigate trust-exploitation attacks. All servers in this module have HIDS installed, and all traffic flows within the module are inspected by the on-board IDS blades in the Layer 3 switches. High availability is ensured through the use of multiple call-processing managers and multiple firewalls configured in high-availability mode. To support the secure management model in the SAFE Enterprise design and the use of an out-of-band management network, all key servers in this module have multiple network interfaces to support the out-of-band access.

Design Alternative for the Large IP Telephony Network

As in the medium-sized network design, you can place the voice-mail server on an additional DMZ interface off the firewall, to further isolate this server and stateful inspection and the filtering of the traffic between the IP telephony devices and the voice-mail server. However, this increases the complexity of the design.

Foundation Summary

The "Foundation Summary" section of each chapter lists the most important facts from the chapter. Although this section does not list every fact from the chapter that will be on your CCSP exam, a well-prepared CCSP candidate should, at a minimum, know all the details in each "Foundation Summary" section before going to take the exam.

The SAFE IP telephony design fundamentals are listed here:

- 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

These axioms have been developed for SAFE IP telephony:

- Voice networks are targets.
- Data and voice segmentation is key.
- Telephony devices do not support confidentiality.
- IP phones provide access to the data-voice segments.
- PC-based IP phones require open access.
- PC-based IP phones are especially susceptible to attack.
- Controlling the voice-to-data segment interaction is key.
- Establishing identity is key.
- Rogue devices pose serious threats.
- Secure and monitor all voice servers and segments.

Table 19-6 shows the key devices in the IP telephony Campus module.

Table 19-6 *Key Devices in Medium-Sized IP Telephony Campus Module*

Key Device	Functions
Layer 3 switch	Routes and switches voice and data traffic within the module.
Layer 2 switch (with VLAN support)	Provides network connectivity to endpoint user workstations and IP phones.
Corporate servers	Provide e-mail and voice-mail services to internal users and provide file, print, and DNS resolution to workstations.
User workstation	Provides data services and voice services (through PC-based IP phones) to end users.
NIDS appliance	Provides Layer 4 to Layer 7 packet inspection.
IP phones	Provides voice services to end users.
Call-processing manager	Provides voice services to IP telephony devices in the module.
Proxy server	Provides data services to IP phones.
Stateful firewall	Provides network-level filtering for the call-processing manager and the proxy server.

Table 19-7 shows the key devices in the large IP telephony Building module.

Table 19-7 *Key Devices in Large IP Telephony Building Module*

Key Device	Functions
Layer 2 switch (with VLAN support)	Provides network connectivity to endpoint user workstations and IP phones.
User workstation	Provides data services and voice services (through PC-based IP phones) to end users.
IP phones	Provide voice services to end users.

Table 19-8 shows the key devices in the large IP telephony Server module.

Table 19-8 *Key Devices in Large IP Telephony Server Module*

Key Device	Functions
Layer 3 switch	Routes and switches voice and data traffic within the module.
Corporate servers	Provide e-mail and voice-mail services to internal users, and provide file, print, and DNS resolution to workstations.
Call-processing manager	Provides voice services to IP telephony devices in the module.
Proxy server	Provides data services to IP phones.
Stateful firewall	Provides network-level filtering for the call-processing manager and the proxy server.

Q&A

As mentioned in the introduction, "All About the Cisco Certified Security Professional Certification," you have two choices for review questions. The questions that follow give you a bigger challenge than the exam itself by using an open-ended question format. By reviewing now with this more difficult question format, you can exercise your memory better and prove your conceptual and factual knowledge of this chapter. The answers to these questions are found in Appendix A.

For more practice with examlike question formats, including questions using a router simulator and multiple-choice questions, use the exam engine on the CD-ROM.

1. What systems are in the Campus module of the small IP telephony blueprint?
2. Why do PC-based IP phones violate the axiom "Data and voice segmentation is key"?
3. What considerations given to production servers in the data segment also should be provided to the voice servers in the voice segment?
4. What is the best way to control the voice and data segment interaction?
5. What are some of the specific attack-mitigation details that are especially applicable to an IP telephony deployment?
6. What are some of the services provided by the voice-enabled firewall/router in the Corporate Internet module of the small IP telephony design?
7. What are the key network devices in the Campus module of the medium-sized IP telephony blueprint, and what are their functions?
8. What is the primary function of the Campus module of the medium-sized IP telephony blueprint?
9. What is the purpose of placing a NIDS between the voice and data segments of the network?
10. How is resiliency provided in the Server module of the large IP telephony design?