CCNA Security Quick Reference

Anthony Sequeira

Your Short Cut to Knowledge

ciscopress.com

About the Author

Anthony Sequeira, CCIE No. 15626, completed the CCIE in Routing and Switching in January 2006. He is currently pursuing the CCIE in Security. For the past 15 years, he has written and lectured to massive audiences about the latest in networking technologies. He is currently a senior technical instructor and certified Cisco Systems instructor for SkillSoft. He lives with his wife and daughter in Florida. When he is not reading about the latest Cisco innovations, he is exploring the Florida skies in a Cessna.

About the Technical Editor

Ryan Lindfield is an instructor and network administrator with Boson. He has more than 10 years of network administration experience. He has taught many courses designed for CCNA, CCNP, and CCSP preparation, among others. He has written many practice exams and study guides for various networking technologies. He also works as a consultant, where among his tasks are installing and configuring Cisco routers, switches, VPNs, intrusion detection systems, and firewalls.

 Please see page 88 for more details.

Network Security Fundamentals

This section covers the need for network security and the security objectives found with most organizations. This section also examines the different types of attacks that modern networks can experience.

Why do we need network security?

Network threats include internal and external threats. Internal threats are the most serious. These threats often occur because best practices are not followed. For example, blank or default passwords are used, or in-house developers use insecure programming practices.

External threats typically rely on technical methods to attack the network. The CCNA in Security focuses on combating these attacks using technical means. Firewalls, routers with access control lists (ACL), intrusion prevention systems (IPS), and other methods are the focus.

Network security objectives

Network security should provide the following:

- Data confidentiality
- Data integrity
- Data and system availability

Confidentiality ensures that only authorized individuals can view sensitive data. Powerful methods of ensuring confidentiality are encryption and access controls.

Integrity ensures that data has not been changed by an unauthorized individual.

 Please see page 88 for more details.

Availability ensures that access to the data is uninterrupted. Denial-of-service (DoS) attacks attempt to compromise data availability. These attacks typically try to fail a system using an unexpected condition or input, or fail an entire network with a large quantity of information.

Data classification

Public-sector classification levels include the following:

- Unclassified
- Sensitive but unclassified (SBU)
- Confidential
- Secret
- Top-secret

Private-sector classification levels include the following:

- Public
- Sensitive
- Private
- Confidential

Classification criteria include the following:

- **Value**: The most important factor.
- **Age**: With time, the sensitivity of data typically decreases.

 Please see page 88 for more details.

- **Useful life**: Information can be made obsolete with newer info.
- **Personal association**: The data is associated with sensitive issues or individuals.

Classification roles include the following:

- Owner
- Custodian (responsible for the day-to-day management of the data)
- User

Security controls

Administrative controls involve policies and procedures.

Technical controls involve electronics, hardware, and software.

Physical controls are mostly mechanical.

Controls are categorized as preventative, deterrent, or detective.

Responses

Investigators must prove motive, opportunity, and means.

The system should not be shut down or rebooted before the investigation begins.

 Please see page 88 for more details.

Laws and ethics

Security policy must attempt to follow criminal, civil, and administrative law.

Ethics refer to values that are even higher than the law.

Network Attack Methodologies

It is very important to understand the command types of attacks that a network can experience. Studying these attacks is the first step in defending against them

Motivations and classes of attack

A vulnerability is a weakness in a system that can be exploited by a threat.

A risk is the likelihood that a specific attack will exploit a particular vulnerability of a system.

An exploit happens when computer code is developed to take advantage of a vulnerability.

The main vulnerabilities of systems are categorized as follows:

- Design errors
- Protocol weaknesses
- Software vulnerabilities
- Misconfiguration

 Please see page 88 for more details.

- Hostile code
- Human factor

Potential adversaries can include the following:

- Nations or states
- Terrorists
- Criminals
- Hackers
- Corporate competitors
- Disgruntled employees
- Government agencies

Many different classifications are assigned to hackers, including the following:

- **Hackers**: Individuals who break into computer networks and systems to learn more about them.
- **Crackers** (criminal hackers): Hackers with a criminal intent to harm information systems.
- **Phreakers** (phone breakers): Individuals who compromise telephone systems.
- **Script kiddies**: Individuals with very low skill level. They do not write their own code. Instead, they run scripts written by other, more skilled attackers.
- **Hacktivists**: Individuals who have a political agenda in doing their work.
- **Academic hackers**: People who enjoy designing software and building programs with a sense for aesthetics and playful cleverness.

 Please see page 88 for more details.

- **Hobby hacker**: Focuses mainly on computer and video games, software cracking, and the modification of computer hardware and other electronic devices.

How does a hacker usually think?

1. Perform footprint analysis (reconnaissance).
2. Enumerate applications and operating systems.
3. Manipulate users to gain access.
4. Escalate privileges.
5. Gather additional passwords and secrets.
6. Install back doors.
7. Leverage the compromised system.

Defense in depth

The defense-in-depth strategy recommends several principles:

- Defend in multiple places.
- Defend the enclave boundaries.
- Defend the computing environment.
- Build layered defenses.
- Use robust components.

 Please see page 88 for more details.

- Use robust key management.
- Deploy IDS or IPS.

IP spoofing

IP spoofing refers to forging the source address information of a packet so that the packet appears to come from some other host in the network. IP spoofing is often the first step in the abuse of a network service, or a DoS type of attack.

In IP spoofing, the attacker sends messages to a computer with an IP address that indicates the message is coming from a trusted host.

The basis of IP spoofing lies in an inherent security weakness in TCP known as sequence prediction. Hackers can guess or predict the TCP sequence numbers that are used to construct a TCP packet without receiving any responses from the server. Their prediction allows them to spoof a trusted host on a local network.

IP spoofing attacks are categorized in one of two ways:

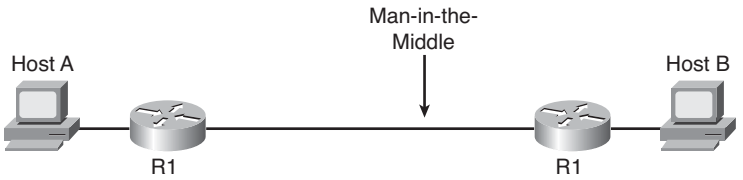
- **Nonblind spoofing**: The attacker sniffs the sequence and acknowledgment numbers and does not need to "predict" them.
- **Blind spoofing**: The attacker sends several packets to the target machine to sample sequence numbers and then predicts them for the attack.

Spoof attacks are often combined with IP source-routing options set in packets. Source routing is the ability of the source to specify within the IP header a full routing path between endpoints. Cisco IOS routers drop all source-routed packets if the **no ip source-route** global command is configured. Security devices, such as Cisco PIX 500 Series Security Appliances and the Cisco ASA 5500 Series Adaptive Security Appliances, drop such packets by default.

 Please see page 88 for more details.

Man-in-the-middle attacks are often the result of TCP/IP spoofing. Figure 1-1 shows a man-in-the-middle attack. An attacker sniffs to identify the client and server IP addresses and relative port numbers. The attacker then modifies his or her packet headers to spoof TCP/IP packets from the client. The attacker waits to receive an ACK packet from the client communicating with the server. The ACK packet contains the sequence number of the next packet that the client is expecting. The attacker replies to the client using a modified packet with the source address of the server and the destination address of the client. This packet results in a reset that disconnects the legitimate client. The attacker takes over communications with the server by spoofing the expected sequence number from the ACK that was previously sent from the legitimate client to the server.

FIGURE 1-1
Man-in-the-middle attack



Confidentiality attacks

Attackers can use many methods to compromise confidentiality. The following are some of the common methods:

- **Packet sniffing**: Eavesdropping and logging traffic that passes over a digital network or part of a network.
- **Port scanning**: Searching a network host for open ports.
- **Dumpster diving**: Searching through company dumpsters, looking for information that can provide a valuable source of information for hackers.
- **Emanations capturing**: Capturing electrical transmissions from the equipment of an organization to obtain information about the organization.
- **Wiretapping**: Monitoring the telephone or Internet conversations of a third party.

 Please see page 88 for more details.

- **Social engineering**: Using social skills to manipulate people inside the network to provide the information needed to access the network.
- **Overt channels**: The ability to hide information within a transmission channel that is based on tunneling one protocol inside another. Steganography is an example of an overt channel: hiding messages in digital pictures and digitized audio.
- **Covert channels**: The ability to hide information within a transmission channel that is based on encoding data using another set of events.
- **Phishing, pharming, and identity theft**: Phishing is an attempt to criminally acquire sensitive information, such as usernames, passwords, and credit card details, by masquerading as a trustworthy entity. Pharming is an attack aimed at redirecting the traffic of one website to another website.

Integrity attacks

Hackers can use many types of attacks to compromise integrity:

- **Salami attacks**: A series of minor data security attacks that together result in a larger attack.
- **Data diddling**: Changing data before or as it is input into a computer.
- **Trust exploits**: An individual taking advantage of a trust relationship within a network. Perhaps the trust relationship is between a system in the DMZ and a system in the inside network.
- **Password attacks**: Any attack that attempts to identify a user account, password, or both.
- **Session hijacking**: The exploitation of a valid computer session to gain unauthorized access to information or services in a computer system.

 Please see page 88 for more details.

Availability attacks

Hackers can use many types of attacks to compromise availability:

- **Botnets**: A collection of software robots that run autonomously and automatically.
- **DoS**: A denial-of-service attack seeks to make a system or service unavailable after the system is sent large amounts of traffic.
- **DDoS** (Distributed DoS): Hackers use a terminal to scan for systems to hack. The hacker then installs zombie software on them.
- **SYN floods**: Here the system is sent many different false SYN requests for TCP communication channels. This is a form of DoS.
- **ICMP floods**: Here the system is sent many false ICMP packets.
- **Electrical power**: Attacks involve power loss, reduction, or spikes.
- **Computer environment**: Temperature, airflow, humidity, water, gas.

Best practices for mitigation

These include the following:

- Keep patches up-to-date.
- Shut down unnecessary services and ports.
- Use strong passwords, and change them often.
- Control physical access to systems.
- Avoid unnecessary web page inputs.

- Perform backups and test the backed-up files on a regular basis.
- Educate employees about the risks of social engineering.
- Encrypt and password-protect sensitive data.
- Implement security hardware and software.
- Develop a written security policy for the company.

Operation Security

Secure network life cycle management

A general system development life cycle (SDLC) includes five phases:

- **Initiation**: Consists of a security categorization and a preliminary risk assessment.
- **Acquisition and development**: Includes a risk assessment, security functional requirements analysis, security assurance requirements analysis, cost considerations and reporting, security planning, security control development, developmental security test and evaluation, and other planning components.
- **Implementation**: Includes inspection and acceptance, system integration, security certification, and security accreditation.
- **Operations and maintenance**: Includes configuration management and control, and continuous monitoring.
- **Disposition**: Includes information preservation, media sanitization, and hardware and software disposal.

 Please see page 88 for more details.

Security testing

Many types of testing techniques are available:

- Network scanning
- Vulnerability scanning
- Password cracking
- Log review
- Integrity checkers
- Virus detection
- War dialing
- War driving (802.11 or wireless LAN testing)
- Penetration testing

The following list is a collection of popular tools:

- Nmap
- GFI LANguard
- Tripwire
- Nessus
- Metasploit
- SuperScan by Foundstone, a division of McAfee

 Please see page 88 for more details.

Disaster recovery

Possible disruptions can be categorized as follows:

- **Nondisaster**: A situation in which business operations are interrupted for a relatively short period of time.
- **Disasters**: Cause interruptions of at least a day.
- **Catastrophe**: The facilities are destroyed, and all operations must be moved.

Backups

- **Hot site**: A completely redundant site, with very similar equipment to the original site
- **Warm site**: A facility that has very similar equipment to the original site, but unlikely to have current data because of a lack of frequent replication with the original site
- **Cold site**: Does not typically contain redundant computing equipment (for example, servers and routers)

Developing a Network Security Policy

This section details the creation of a network security policy—a very important document that details the security objectives and procedures for the organization.

 Please see page 88 for more details.

Why do you need one?

Aside from protecting organization assets, a security policy serves other purposes, such as the following:

- Making employees aware of their security-practice obligations
- Identifying specific security solutions required to meet the goals of the security policy
- Acting as a baseline for ongoing security monitoring

Components of the security policy

What are the exact components found in the network security policy? This section covers those details.

Governing policy

At a very high level, a governing policy addresses security concepts deemed important to an organization. Here are typical elements of this section:

- Identification of the issue addressed by the policy
- Discussion of the organization's view of the issue
- Examination of the relevance of the policy to the work environment
- Explanation of how employees are to comply with the policy
- Enumeration of appropriate activities, actions, and processes
- Explanation of the consequences of noncompliance

 Please see page 88 for more details.

Technical policies

Technical policies provide a more detailed treatment of an organization's security policy, as opposed to the governing policy. Elements of this section include the following:

- E-mail
- Wireless networks
- Remote access

End-user policies

End-user policies address security issues and procedures relevant to end users.

More detailed documents

More detailed documents are often contained in a security policy:

- **Standards**: Support consistency within a network.
- **Guidelines**: Tend to be suggestions.
- **Procedures**: Detailed documents providing step-by-step instructions for completing specific tasks.

Roles and responsibilities

The ultimate responsibility for an organization's security policy rests on the shoulders of senior management. Senior management typically oversees the development of a security policy. Senior security or IT personnel are

 Please see page 88 for more details.

usually directly involved with the creation of the security policy. Examples of senior security or IT personnel include the following:

- Chief security officer (CSO)
- Chief information officer (CIO)
- Chief information security officer (CISO)

Risk analysis, management, and avoidance

Network designers identify threats to the network using threat identification practices. Also, analysis must be performed of the probability that a threat will occur and the severity of that threat. This is risk analysis. When performing risk analysis, one of two approaches can be used:

- **Quantitative analysis**: Mathematically models the probability and severity of a risk. A sample quantitative analysis formula is ALE = AV * EF * ARO; this formula calculates the annualized loss expectancy (ALE). The ALE produces a monetary value that can be used to help justify the expense of security solutions. AV is asset value, EF is the exposure factor, and ARO is the annualized rate of occurrence.
- **Qualitative analysis**: Uses a scenario model, where scenarios of risk occurrence are identified.

Creating the Cisco Self-Defending Network

This type of network is built in three phases:

- **Integrated**: Every element is a point of defense.
- **Collaborative**: Collaboration among the service and devices throughout the network.
- **Adaptive**: The network can intelligently evolve and adapt the threats.

 Please see page 88 for more details.

Benefits

- Reduced integration costs
- Proactive, planned upgrades
- Improves efficiency of security management

Key tools

- **Cisco Security Manager**: Powerful but easy-to-use solution that enables you to centrally provision all aspects of device configurations and security policies for the Cisco family of security products.
- **MARS** (Cisco Security Monitoring, Analysis, and Response System): Provides security monitoring for network security devices and host applications made by Cisco and other providers.

 Please see page 88 for more details.

Securing Administrative Access to Routers

It is critical to secure administrative access to the routers that help power your network infrastructure. This section details exactly how this should be carried out.

Router security principles

There are three areas of router security:

- Physical security
- Operating system
- Router hardening

Cisco Integrated Services Router family

Cisco Integrated Services Routers feature comprehensive security services, embedding data, security, voice, and wireless in the platform portfolio for fast, scalable delivery of mission-critical business applications. Models include the 800 Series, 1800 Series, 2800 Series, and 3800 Series.

Configuring secure administrative access

You need to secure administrative access for local access (console port) and remote access such as HTTP or Telnet/SSH.

 Please see page 88 for more details.

Be sure to password-protect your router. These commands can be used:

- Console password

```
line console 0
login
password cisco
```

- Virtual terminal password

```
line vty 0 4
login
password cisco
```

- Enable password

```
enable password cisco
```

- Secret password

```
enable secret cisco
```

All these passwords are in clear text in the configuration files with the exception of the **enable secret** command. To encrypt the passwords that are clear text, use the command **service password-encryption**.

To configure idle timeouts for router lines, use the command **exec-timeout** *minutes* [*seconds*].

You can also configure minimum password lengths with the **security passwords min-length** *length* command.

To create username and password entries in the local accounts database, use the syntax **username** *name* **secret** {[**0**] *password* | **5** *encrypted-secret*}.

 Please see page 88 for more details.

To disable the ability to access ROMMON to disable password recovery on your router, use **no service password-recovery**.

Setting multiple privilege levels

You can configure multiple privilege levels on the router for different levels of your administrators. There are 16 privilege levels, 0 to 15. Level 0 is reserved for user-level access privileges, levels 1 to 14 are levels you can customize, and level 15 is reserved for privileged mode commands. To assign privileges to levels 2 to 14, use the **privilege** command from global configuration mode. The syntax for this command is **privilege mode** {**level** *level command* | **reset** *command*}. Remember that privilege levels are "cascading." If a user has level 13 access, that user also gains access to the commands in levels 1 through 12.

Role-based CLI access

A new approach to having various levels of access for different administrators is called role-based CLI access. Using this approach, different administrators have different "views" of the CLI. These views contain the specific commands that are available for different administrators. To configure role-based CLI, complete the following steps:

Step 1. Enable AAA.

Step 2. Use the **enable view** command to enable the feature.

Step 3. Use the **configure terminal** command to enter global configuration mode.

Step 4. Use the **parser view** *view-name* command to create a new view.

Step 5. Use the **secret** command to assign a password to the view.

 Please see page 88 for more details.

Step 6. Use the command **commands** *parser-mode* {**include** | **include-exclusive** | **exclude**} [**all**] [**interface** *interface-name* | *command*] to assign commands to the selected view.

Step 7. Verify using the **enable view** command.

Securing the Cisco IOS image and configuration files

You can now secure copies of the IOS and your configuration file in memory so that they cannot be maliciously or accidentally erased. The **secure boot-image** command protects the IOS image, and the command **secure boot-config** protects the running configuration. These protected files will not even appear in a **dir** listing of flash. To see these protected files, use the **show secure bootset** command.

Enhanced security for virtual logins

The following commands have been added to enhance security for virtual logins:

- **login block-for** *seconds* **attempts** *tries* **within** *seconds*

  This command configures your Cisco IOS device for login parameters that help provide denial-of-service (DoS) detection. This command is mandatory; all other commands here are optional.

- **login quiet-mode** *access-class* {*acl-name* | *acl-number*}

  This command specifies an ACL that is to be applied to the router when it switches to quiet mode. The devices that match a **permit** statement in the ACL are exempt from the quiet period.

- **login delay** *seconds*

  Configures a delay between successive login attempts.

- **login on-failure log** [**every** *login*]

  Generates logging messages for failed login attempts.

 Please see page 88 for more details.

- **login on-success log** [**every** *login*]

  Generates logging messages for successful login attempts.

- **show login**

  Verifies that the **login block-for** command is issued.

Banner messages

Banner messages are important. With these messages, you can ensure that unauthorized personnel are informed that they will be prosecuted for illegal access. The syntax for this command is **banner** {**exec** | **incoming** | **login** | **motd** | **slip-ppp**} *d message d*.

Cisco Security Device Manager (SDM)

SDM is a powerful graphical user interface you can use to configure and monitor your Cisco router.

Supporting SDM

Cisco SDM is factory-installed on some router models. It is also available on a CD-ROM that is included with new routers, and it can be downloaded from Cisco.com. In addition to the full SDM, an SDM Express version is available.

If the router is an existing router and is not configured with the Cisco SDM default configuration, configure the following services for Cisco SDM to access the router properly:

- Set up a username and password that has privilege level 15:

```
username name privilege 15 secret password
```

 Please see page 88 for more details.

- Enable the HTTP server:

```
ip http server
ip http authentication local
ip http secure-server (for enabling HTTPS access to Cisco SDM)
ip http timeout-policy idle 600 life 86400 request 1000
```

- Define the protocol to use to connect to the Telnet and Secure Shell (SSH) vty lines:

```
line con 0
login local
line vty 0 4
privilege level 15
login local
transport input telnet ssh
line vty 5 15
privilege level 15
login local
transport input telnet ssh
```

On a new router, you can access Cisco SDM Express from your PC web browser by going to http://10.10.10.1.

Running SDM

To launch Cisco SDM from a PC, choose **Start > Programs (All Programs) > Cisco Systems > Cisco SDM > Cisco SDM**.

To launch Cisco SDM from the router flash memory, open an HTTP or HTTPS connection to the IP address of the Ethernet interface on the router.

 Please see page 88 for more details.

Navigating in SDM

Home, **Configure**, and **Monitor** are the main buttons you will use. These appear on the top button bar. When you click either **Configure** or **Monitor**, many options appear down the button bar on the left side of the screen. Many of these options lead to a wizard that aids in the configuration.

Using AAA with the Local Database

AAA (Authentication, Authorization, and Accounting) services are a powerful security addition to any organization. This section details the use of these services in conjunction with a local database on the router or switch.

Authentication, authorization, and accounting

Authentication requires users and administrators to prove that they really are who they say they are. Authorization dictates what these users can do after they are authenticated. Accounting tracks what users do.

AAA can be used to control administrative access to the device and access to the network beyond through the device.

Cisco provides four methods for implementing AAA:

- Self-contained AAA using the local database
- Cisco Secure Access Control Server (ACS) for Microsoft Windows Server
- Cisco Secure ACS Express (entry-level version appropriate for 350 users)
- Cisco Secure ACS Solution Engine (rack-mountable hardware version)

 Please see page 88 for more details.

Local authentication

Using this method, the user connects to the router, the router prompts for a username and password, and then the router authenticates using the local database. There are two modes: character mode (when the user is trying to connect to the router for admin), and packet mode 0 (when the user is trying to connect through the router for access to the network beyond).

To configure in SDM, choose **Configure > Additional Tasks > Router Access > User Accounts/View** to add user accounts. Then choose **Configure > Additional Tasks > AAA** to ensure that AAA is enabled. Then choose **Configure > Additional Tasks > AAA > Authentication Policies > Login** to configure the local setting.

Additional settings can be made at the command line. For example, to specify the maximum number of unsuccessful authentication attempts before a user is locked out, use the **aaa local authentication attempts max-fail** command in global configuration mode. To display a list of all locked-out users, use the **show aaa local user lockout** command in privileged EXEC mode. Use the **clear aaa local user lockout** command in privileged EXEC mode to unlock a locked-out user. To display the attributes that are collected for a AAA session, use the **show aaa user** {**all** | **unique id**} command in privileged EXEC mode. You can use the **show aaa sessions** command to show the unique ID of a session. To display information about AAA authentication, use the **debug aaa authentication** command in privileged EXEC command mode.

SDM creates the necessary commands at the CLI from the GUI. SDM uses the following commands on the router:

- The **aaa new-model** command enables AAA.
- The **aaa authentication login default local** command defines the default method list for login authentication using the local database.
- The **username** command adds a username and password to the local security database.

 Please see page 88 for more details.

Using AAA with Cisco Secure ACS

ACS is a more scalable solution than trying to create and maintain user accounts on separate Cisco devices.

To communicate with the external Cisco Secure ACS, the Cisco device uses TACACS+ or RADIUS. Of the two, TACACS+ is more secure, but RADIUS is an open standard. Also, many of the most modern security features require the use of the open-standard RADIUS protocol.

TACACS+ offers the following features:

- Separates authentication and authorization
- Supports a large number of features
- Encrypts all communications
- Uses TCP port 49

RADIUS offers the following features:

- Scales well
- Uses UDP ports 1645 or 1812 for authentication and UDP ports 1646 or 1813 for accounting

To configure the router for AAA with ACS, use SDM and choose **Configure > Additional Tasks > AAA > AAA Servers and Groups > AAA Servers** and add the servers. Then choose **Configure > Additional Tasks > AAA > Authentication Policies > Login** to create a policy. You can apply a policy that you create using **Configure > Additional Tasks > Router Access > VTY**.

 Please see page 88 for more details.

Implementing Secure Management and Reporting

Management traffic is often a necessity in the network infrastructure. This section details how to ensure that this traffic does not represent a security breach.

The architecture for secure management and reporting

The information flow between management hosts and the managed devices can take two paths:

- **Out-of-band (OOB)**: Information flows within a network on which no production traffic resides.
- **In-band**: Information flows across the enterprise production network.

Overall guidelines for secure management and reporting include the following:

- Keep clocks on hosts and network devices synchronized.
- Record changes and archive configurations.

OOB management guidelines

- Help ensure that management traffic is not intercepted on the production network.

In-band management guidelines

- Apply only to those devices that truly need to be managed in this manner.
- Use IPsec, SSH, or SSL.
- Decide whether monitoring needs to be constant or periodic.

 Please see page 88 for more details.

Syslog

Syslog is the current standard for logging system events in a Cisco infrastructure. It is the most popular option for storing Cisco router log messages. The Cisco Security Monitoring, Analysis, and Response System (MARS) is a Cisco security appliance that can receive and analyze syslog messages from various networking devices and hosts.

Remember that router log messages can also be sent to

- The console
- Terminal lines
- An internal buffer
- SNMP traps

Figure 2-1 shows the various Cisco log severity levels.

Cisco router log messages contain three main parts:

- Time stamp
- Log message name and severity level
- Message text

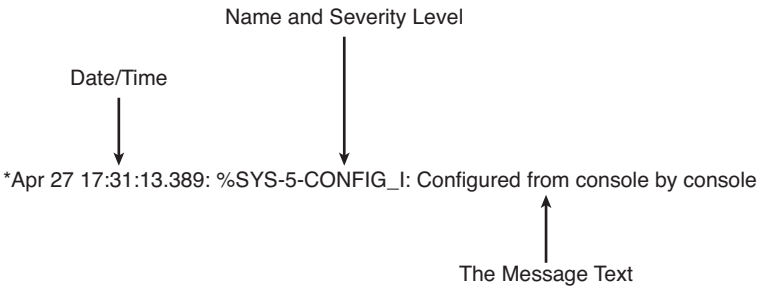
Figure 2-2 shows this message format.

 Please see page 88 for more details.

FIGURE 2-1
Cisco log severity levels

Level	Name	Description
0	Emergencies	A panic condition normally broadcast to all users
1	Alerts	A condition that should be corrected immediately, such as a corrupted system database
2	Critical	Critical conditions; for example, hard device errors
3	Errors	Errors
4	Warnings	Warning messages
5	Notifications	Conditions that are not error conditions, but should possibly be handled specially
6	Information	Informational messsages
7	Debugging	Messages that contain information normally of use only when debugging a program

FIGURE 2-2
Cisco log message format



To enable syslog logging on your router using SDM, choose **Configure > Additional Tasks > Router Properties > Logging**. To view the syslog information, choose **Monitor > Logging**.

Simple Network Management Protocol (SNMP)

Versions 1 and 2c of SNMP use clear-text passwords called community strings. This offers little to no security.

SNMP 3 uses a combination of authenticating and encrypting packets over the network to provide secure access to devices. SNMP 3 provides message integrity, authentication, and encryption.

SNMP 3 supports all three of the following security levels:

- **noAuth**: Community string
- **auth**: HMAC or MD5 (hashing for integrity)
- **Priv**: DES, 3DES, or AES (encryption for confidentiality)

When actually implemented on a router, these levels can be combined. For example, authPriv allows the use of authentication and encryption.

To use the SDM to configure SNMP, choose **Configure > Additional Tasks > Router Properties > SNMP**.

SSH

The SSH daemon is a feature that enables an SSH client to make a secure, encrypted connection to a Cisco router. Use SSH rather than Telnet to manage Cisco devices. Cisco IOS Release 12.1(1)T and later support SSH Version 1 (SSHv1), and Cisco IOS Release 12.3(4)T and later support both SSHv1 and SSH Version 2 (SSHv2). The Cisco router acts as the SSH server, and the client must be acquired to connect to the server. A sample client is PuTTY.

 Please see page 88 for more details.

To use SDM to configure SSH, choose **Configure > Additional Tasks > Router Access > SSH**.

After enabling SSH on the router, configure the vty lines to support SSH. To use Cisco SDM to configure SSH on the vty lines, choose **Configure > Additional Tasks > Router Access > VTY**.

To use the command line for the configuration, follow these steps:

Step 1. Configure the IP domain name of your network using the **ip domain-name** *domain-name* command in global configuration mode.

Step 2. If there are any existing key pairs, it is recommended that you overwrite them using the command **crypto key zeroize rsa**.

Step 3. Generate keys to be used with SSH by generating RSA keys using the **crypto key generate rsa general-keys modulus** *modulus-size* command in global configuration mode.

Step 4. Configure how long the router waits for the SSH client to respond using the **ip ssh timeout** *seconds* command in global configuration mode; this step is optional.

Step 5. Configure the number of SSH retries using the **ip ssh authentication-retries** *integer* command in global configuration mode; this step is optional.

Step 6. Enable vty inbound SSH sessions; use the **transport input ssh** command.

Time features

You can use Cisco SDM to configure the date and time settings of the router in three ways:

- Synchronize with the local PC clock
- Manually edit the date and time
- Configure NTP (Network Time Protocol)

 Please see page 88 for more details.

To do this in SDM, choose **Configure > Additional Tasks > Router Properties > Date/Time**. For an NTP configuration, choose **Configure > Additional Tasks > Router Properties > NTP/SNTP**.

Locking Down the Router

Cisco provides two powerful methods for locking down the router. This means disabling or protecting unused services, and making other configuration changes that are necessary for a secure network infrastructure.

AutoSecure

The AutoSecure IOS feature is invoked by issuing the **auto secure** command from the CLI.

Cisco SDM One-Step Lockdown

The Cisco SDM One-Step Lockdown method for securing a router uses a wizard in the Cisco SDM graphical interface. To access this feature, choose **Configure > Security Audit**. Note that there is also a very informative Security Audit feature you can use before performing the One-Step Lockdown.

You should keep in mind some distinctions between the two approaches:

- One-Step Lockdown does not support the disabling of NTP.
- One-Step Lockdown does not support the configuration of AAA.
- One-Step Lockdown does not support the setting of Selective Packet Discard (SPD) values.
- One-Step Lockdown does not support the enabling of TCP intercepts.
- One-Step Lockdown does not configure antispoofing access control lists.

 Please see page 88 for more details.

- Although One-Step Lockdown does support the disabling of SNMP, it does not support the configuration of SNMP 3.
- Although One-Step Lockdown does support the configuration of SSH access, it does not support the enabling of Service Control Point or the disabling of other access services and file transfer services.

 Please see page 88 for more details.

Firewall Technologies

Firewalls are a key security technology in the modern network infrastructure. This section details their evolution and the technologies that have resulted.

Firewall fundamentals

The firewall should

- Be resistant to attacks
- Be the only transit point
- Enforce the access control policy of the organization

Static packet-filtering firewalls

These work at Layer 3 and 4, examining packets one at a time. They are implemented on a Cisco router using access control lists (ACL).

Advantages of these firewalls include the following:

- Are based on simple **permit** and **deny** sets
- Low impact on network performance
- Easy to implement
- Supported on most routers
- Initial security at a low network layer
- Perform most of what higher-end firewalls do at a lower cost

 Please see page 88 for more details.

Disadvantages of these firewalls include the following:

- Susceptible to IP spoofing.
- Packet filters do not filter fragmented packets well.
- Complex ACLs are difficult to implement and maintain correctly.
- Packet filters cannot dynamically filter certain services.
- Packet filters are stateless; they do not maintain any state information for added protection.

Application layer gateways

Application layer firewalls (also called proxy firewalls or application gateways) operate at Layers 3, 4, 5, and 7 of the OSI model. Proxy services are specific to the protocol that they are designed to forward, and they can provide increased access control, provide careful detailed checks for valid data, and generate audit records about the traffic they transfer. Sometimes, application layer firewalls support only a limited number of applications.

Application layer firewalls offer advantages:

- Authenticate individuals, not devices
- Make it harder for hackers to spoof and implement denial-of-service (DoS) attacks
- Can monitor and filter application data
- Can provide detailed logging

The disadvantages are as follows:

- Process packets in software
- Support a small number of applications

 Please see page 88 for more details.

- Sometimes require special client software
- Are memory- and disk-intensive

Dynamic or stateful packet-filtering firewalls

Stateful inspection is a firewall architecture that is classified at the network layer, although for some applications it can analyze traffic at Layers 4 and 5, too.

Unlike static packet filtering, stateful inspection tracks each connection traversing all interfaces of the firewall and confirms that they are valid. Stateful packet filtering maintains a state table and allows modification to the security rules dynamically. The state table is part of the internal structure of the firewall. It tracks all sessions and inspects all packets passing through the firewall.

Although this is the primary Cisco firewall technology, it has some limitations:

- Cannot prevent application layer attacks.
- Not all protocols are stateful.
- Some applications open multiple connections.
- Does not support user authentication.

Other types

Application inspection firewalls ensure the security of applications and services. Advantages include the following:

- Are aware of the state of Layer 4 and Layer 5 connections
- Check the conformity of application commands at Layer 5

 Please see page 88 for more details.

- Can and affect Layer 7
- Can prevent more kinds of attacks than stateful firewalls can

Transparent firewalls (Cisco PIX and Cisco Adaptive Security Appliance Software Version 7.0) can deploy a security appliance in a secure bridging mode as a Layer 2 device to provide security services at Layer 2 to Layer 7.

Cisco Firewall family

Cisco IOS Firewall features

- Zone-based policy framework for intuitive policy management
- Application firewalling for web, e-mail, and other traffic
- Instant messenger and peer-to-peer application filtering
- VoIP protocol firewalling
- Virtual routing and forwarding (VRF) firewalling
- Wireless integration
- Stateful failover
- Local URL whitelist and blacklist support; remote server support too, through Websense or SmartFilter

Cisco PIX 500 Series Security Appliance features

- Advanced application-aware firewall services
- Market-leading VoIP and multimedia security
- Robust site-to-site and remote-access IP security (IPsec) VPN connectivity

 Please see page 88 for more details.

- Award-winning resiliency
- Intelligent networking services
- Flexible management solutions

Cisco ASA 5500 Series Adaptive Security Appliance features

- World-class firewall
- Voice and video security
- SSL and IPsec VPN
- IPS
- Content security
- Modular devices
- High scalability

Best practices

Firewall best practices include the following:

- Position firewalls at key security boundaries.
- Firewalls are the primary security device, but it is unwise to rely exclusively on a firewall for security.
- Deny all traffic by default and permit only services that are needed.
- Ensure that physical access to the firewall is controlled.

 Please see page 88 for more details.

- Regularly monitor firewall logs. Cisco Security Monitoring, Analysis, and Response System (MARS) is especially useful in monitoring firewall logs.
- Practice change management.
- Remember that firewalls primarily protect from technical attacks originating from the outside.

Static Packet Filters Using ACLs

Fundamentals of ACLs

ACLs operate in two ways:

- **Inbound ACLs**: Incoming packets are processed before they are routed to an outbound interface.
- **Outbound ACLs**: Incoming packets are routed to the outbound interface, and then they are processed through the outbound ACL.

If there is no matching **permit** or **deny** statement and the entire access list has been processed, the packet is denied by an implicit **deny all** at the end of the access list.

Cisco routers support two types of IP ACLs:

- **Standard ACLs**: Check the source addresses of packets that can be routed.
- **Extended ACLs**: Check both the source and destination packet addresses. They can also check for specific protocols, port numbers, and other parameters.

 Please see page 88 for more details.

You can use two general methods to create ACLs:

- **Numbered ACLs**: Use a number for identification.
- **Named ACLs**: Use an alphanumeric string for identification.

Cisco IOS Release 12.3 or later features IP access list entry sequence numbering to assist in the management of ACLs.

Follow these guidelines with ACLs:

- Based on the test conditions, choose a standard or extended, numbered or named ACL.
- Only one ACL per protocol, per direction, and per interface is allowed.
- Your ACL should be organized to allow processing from the top down. Organize your ACL so that the more specific references to a network or subnet appear before ones that are more general.
- Unless you end your ACL with an explicit **permit any** statement, by default the ACL denies all traffic that fails to match any of the ACL lines.
- Every ACL should have at least one **permit** statement.
- You should create the ACL before applying it to an interface.
- If you apply an ACL to an interface, the ACL filters traffic going through the router but does not filter traffic that the router generates.
- You should typically place extended ACLs as close as possible to the source of the traffic that you want to deny. You must put the standard ACL as close as possible to the destination of the traffic you want to deny.

 Please see page 88 for more details.

ACL wildcard masking

Wildcard masking for IP address bits uses the numerals 1 and 0 to specify how to treat the corresponding IP address bits:

- **Wildcard mask bit 0**: Match the corresponding bit value in the address
- **Wildcard mask bit 1**: Ignore the corresponding bit value in the address

Figure 3-1 shows an example of wildcard masking.

FIGURE 3-1
Wildcard masking

An administrator wants to match the subnets 172.40.16.0/24 to 172.40.31.0/24.

The first two octets of the wildcard mask will be 0.0 since 172.40 must be matched exactly.

For the third octet, the administrator first converts the starting range number to binary:
16 = 0 0 0 1 0 0 0 0

Notice the administrator does not care about the binary values in the last four bit positions; therefore, the wildcard mask is:
0 0 0 0 1 1 1 1 = 15

Also, the administrator does not care at all about any bit in the last octet, so this octet is all 1 values:
1 1 1 1 1 1 1 1 = 255

The resulting address and wildcard mask used in the ACL are:
172.40.16.0 0.0.15.255

You can use abbreviations in your wildcard masks. For example, instead of 0.0.0.0, you can use the keyword **host**. Instead of 255.255.255.255, you can use the keyword **any**.

 Please see page 88 for more details.

ACL creation

To create the standard ACL, use

```
access-list access-list-number {deny ¦ permit} source [source-wildcard]
```

To assign the standard ACL to an interface, use

```
ip access-group {access-list-number ¦ access-list-name}{in ¦ out}
```

To assign an ACL to a vty line, use

```
access-class access-list-number {in [vrf-also] ¦ out}
```

To create an extended ACL, use

```
access-list access-list-number [dynamic dynamic-name [timeout minutes]] {deny ¦ permit} protocol source
source-wildcard destination destination-wildcard [precedence precedence] [tos tos] [log ¦ log-input]
[time-range time-range-name] [fragments] [established]
```

Use the **show access-list** command to verify the ACL, and use **show ip interface** to check for assignment.

The Security Device Manager (SDM) offers an excellent GUI for ACL creation. Choose **Configure > Additional Tasks > ACL Editor > Access Rules**.

Cisco IOS Zone-Based Policy Firewall

One of the most exciting developments for Cisco in the area of IOS firewalls has been the new zone-based firewall. This section details this new technology.

 Please see page 88 for more details.

Overview

With Cisco IOS Release 12.4(6)T, a new configuration model for the Cisco IOS Firewall feature set was introduced. This new model presented the Cisco IOS zone-based policy, which provides the following:

- Intuitive policies for multiple interface routers
- A greater level of granularity for firewall policy application
- The ability to prohibit traffic between firewall zones until an explicit policy is applied to allow desirable traffic via a default deny-all policy

The new zone-based policy inspection interface supports almost all the firewall features implemented in earlier releases and much more, including the following:

- Stateful packet inspection.
- Application inspection.
- Virtual private network (VPN) VRF-aware Cisco IOS Firewall.
- URL filtering.
- DoS mitigation.
- Policies are applied between zones.
- Default deny-all policy.
- Subnet- and host-specific policies.
- Combining service lists with network and host address lists is allowed.
- Clearer statement of firewall policies.
- Unidirectional policy between zones.

 Please see page 88 for more details.

Policies may be made up of combinations of the following:

- IP addresses or subnets using ACLs
- Protocols
- Application services
- Application-specific policies

The zone-based firewall approach takes three possible actions:

- **Inspect**: Causes Cisco IOS stateful packet inspection
- **Drop**: Analogous to a **deny** statement in an ACL
- **Pass**: Analogous to a **permit** statement in an ACL

Configuring the zone-based firewall

To configure a zone-based firewall using the Basic Firewall wizard, choose **Configuration > Firewall and ACL**. From the **Create Firewall** tab, click **Basic Firewall**.

To manually configure a zone-based firewall using the SDM, follow these steps:

Step 1. Define the zones; choose **Configure > Additional Tasks > Zones**.

Step 2. Define class maps; choose **Configure > Additional Tasks > C3PL > Class Map > Inspection**.

Step 3. Define policy maps; choose **Configure > Additional Tasks > C3PL > Policy Map > Protocol Inspection**.

Step 4. Define zone pairs and assign policy maps to them; choose **Configure > Additional Tasks > Zone Pairs**.

 Please see page 88 for more details.

To monitor the firewall in SDM, choose **Monitor > Firewall Status**.

To monitor from the command line, use the **show policy-map type inspect zone-pair session** command.

 Please see page 88 for more details.

Cryptographic Services

This section covers the key topics of cryptography. You should understand these principles before studying VPN technologies.

Overview

Cryptology is the science of making and breaking secret codes. A cipher is an algorithm for performing encryption and decryption. The Vigenère cipher is a polyalphabetic cipher that encrypts text by using a series of different Caesar ciphers based on the letters of a keyword.

Cryptanalysis is the practice of breaking codes to obtain the meaning of encrypted data. Here are examples of attacks:

- **Brute-force attack**: The attacker tries every possible key with the decryption algorithm.
- **A cipher-text-only attack**: The attacker has the cipher text of several messages but no knowledge of the underlying plain text. The attacker must deduce the key or keys used to encrypt the messages to decrypt other messages encrypted with the same keys.
- **A known-plain-text (the usual brute-force) attack**: The attacker has access to the cipher text of several messages but also knows something about the plain text underlying that cipher text. The attacker uses a brute-force attack to try keys until decryption with the correct key produces a meaningful result.
- **A chosen-plain-text attack**: The attacker chooses what data the encryption device encrypts and observes the cipher-text output.
- **A chosen-cipher-text attack**: The attacker can choose different cipher texts to be decrypted and has access to the decrypted plain text.
- **Birthday attack**: A form of brute-force attack against hash functions.
- **Meet-in-the-middle attack**: The attacker knows a portion of the plain text and the corresponding cipher text.

 Please see page 88 for more details.

The following are features that good encryption algorithms provide:

- Resist cryptographic attacks
- Support variable and long key lengths and scalability
- Create an avalanche effect
- Do not have export or import restrictions

Symmetric and asymmetric encryption algorithms

There are two classes of encryption algorithms, which differ in their use of keys:

- **Symmetric encryption algorithms**: Same key to encrypt and decrypt data
- **Asymmetric encryption algorithms**: Different keys to encrypt and decrypt data

The following are well-known encryption algorithms that use symmetric keys:

- **DES**: 56-bit keys
- **Triple Data Encryption Standard (3DES)**: 112- and 168-bit keys
- **AES**: 128-, 192-, and 256-bit keys
- **International Data Encryption Algorithm (IDEA)**: 128-bit keys
- **The RC series**: RC2, RC4, RC5, and RC6
- **RC2**: 40- and 64-bit keys
- **RC4**: 1- to 256-bit keys
- **RC5**: 0- to 2040-bit keys

 Please see page 88 for more details.

- **RC6**: 128-, 192-, and 256-bit keys
- **Blowfish**: 32- to 448-bit keys

Because of their fast speed, symmetric algorithms are frequently used for encryption services, with additional key management algorithms providing secure key exchange.

The best-known asymmetric cryptographic algorithms are

- RSA
- ElGamal
- Elliptic curve algorithms

Block ciphers transform a fixed-length block of plain text into a block of cipher text of the same length. Applying the reverse transformation to the cipher-text block, using the same secret key, results in decryption. Currently, the fixed length, also known as the block size, for many block ciphers is typically 128 bits. DES has a block size of 64 bits.

Unlike block ciphers, stream ciphers operate on smaller units of plain text, typically bits. With a stream cipher, the transformation of these smaller plain-text units varies, depending on when they are encountered during the encryption process. RC4 is a common stream cipher.

Cryptographic hashes

Hashing is a mechanism that is used for data integrity. Data of arbitrary length is input into the hash function, and the result of the hash function is the fixed-length hash.

 Please see page 88 for more details.

Key management

Key management consists of the following components:

- Key generation
- Key verification
- Key storage
- Key exchange
- Key revocation and destruction

SSL VPNs

SSL-based VPNs provide remote-access connectivity from almost any Internet-enabled location using a standard web browser and its native SSL encryption.

The steps of SSL VPN establishment are as follows:

Step 1. The user makes an outbound connection to TCP port 443, typically using a web browser.

Step 2. The router responds with a digital certificate, which contains a public key that is digitally signed by a trusted certificate authority (CA).

Step 3. The user computer generates a shared-secret symmetric key that both parties will use.

Step 4. The shared secret is encrypted with the public key of the router and transmitted to the router. The router software can easily decrypt the packet using its private key. Now both participants in the session know the shared secret key.

Step 5. The key is used to encrypt the SSL session.

 Please see page 88 for more details.

Symmetric Encryption

Symmetric encryption is a common approach to encryption used with VPNs. This section describes this important technology.

Key lengths

Symmetric encryption algorithms typically use keys of length 40 to 256 bits. Lengths of 80 bits or longer are considered trusted.

DES

This encryption algorithm typically operates in block mode, where it encrypts data in 64-bit blocks.

DES uses two standardized block cipher modes:

- **Electronic Code Book (ECB)**: Serially encrypts each 64-bit plain-text block using the same 56-bit key.
- **Cipher Block Chaining (CBC)**: Each 64-bit plain-text block is exclusive ORed (XORed) bitwise with the previous cipher-text block and then is encrypted using the DES key.

Guidelines for DES usage include the following:

- Change keys frequently to help prevent brute-force attacks.
- Use a secure channel to communicate the DES key from the sender to the receiver.
- Use DES in CBC mode.
- Test a key to see whether it is weak before using it.
- Use 3DES rather than DES.

 Please see page 88 for more details.

3DES

The technique of applying DES three times in a row to a plain-text block is called 3DES.

AES

The AES algorithm currently specifies how to use keys with a length of 128, 192, or 256 bits to encrypt blocks with a length of 128, 192, or 256 bits. This provides nine different combinations of key length and block length. Both block length and key length can be extended easily in multiples of 32 bits. AES was chosen to replace DES and 3DES because the key length of AES is much stronger than DES and AES runs faster than 3DES on comparable hardware. AES is more suitable for high-throughput, low-latency environments, especially if pure software encryption is used.

Software-Optimized Encryption Algorithm (SEAL)

SEAL is an alternative algorithm to software-based DES, 3DES, and AES. SEAL encryption uses a 160-bit encryption key and has less impact on the CPU compared to other software-based algorithms.

Restrictions for SEAL include the following:

- The Cisco router and the other peer must support IPsec, and it cannot be hardware-based encryption.
- The Cisco router and the other peer must support the k9 subsystem.

This feature is available only on Cisco equipment.

Rivest ciphers

Widely used RC algorithms include the following:

- **RC2**: A variable key-size block cipher that was designed as a replacement for DES
- **RC4**: A variable key-size Vernam stream cipher that is often used in file-encryption products and for secure communications
- **RC5**: A fast block cipher that has variable block size and variable key size
- **RC6**: A block cipher that was designed by Rivest, Sidney, and that Yin and is based on RC5 (meant to meet the design requirements of AES)

Cryptographic Hashes

This section details the most common cryptographic hashes in use today.

Hash Message Authentication Codes (HMAC)

Hashing is typically used for the following:

- To provide proof of the integrity of data, such as that provided with file integrity checkers, digitally signed contracts, and Public Key Infrastructure (PKI) certificates
- To provide proof of authenticity when it is used with a symmetric secret authentication key, such as IPsec or routing protocol authentication

 Please see page 88 for more details.

Cisco technologies use two HMAC functions:

- Keyed MD5, based on the MD5 hashing algorithm
- Keyed SHA-1, based on the SHA-1 hashing algorithm

Cisco products use hashing for entity-authentication, data-integrity, and data-authenticity purposes:

- IPsec gateways and clients use hashing algorithms to provide packet integrity and authenticity.
- Cisco IOS routers use hashing with secret keys to add authentication information to routing protocol updates.
- Cisco software images have an MD5-based checksum available so that customers can check the integrity of downloaded images.
- Hashing can also be used in a feedback-like mode to encrypt data; TACACS+ uses MD5 to encrypt its session.

MD5

MD5 is a one-way function that makes it easy to compute a hash from the given input data but makes it unfeasible to compute input data given only a hash. The input is a data block plus a feedback of previous blocks. The 512-bit blocks are divided into 16 32-bit subblocks. These blocks are then rearranged with simple operations in a main loop, which consists of four rounds. The output of the algorithm is a set of four 32-bit blocks, which concatenate to form a single 128-bit hash value. The message length is also encoded into the digest.

SHA-1

The SHA-1 algorithm takes a message of no less than 264 bits in length and produces a 160-bit message digest. The algorithm is slightly slower than MD5, but the larger message digest makes it more secure against brute-force collision and inversion attacks. There are also 224-, 256-, 384-, and 512-bit versions of SHA.

 Please see page 88 for more details.

Best practices include the following:

- Avoid MD5 if possible.
- Consider using MD5 only if speed is an issue.
- Protect HMAC secret keys.

Digital Signatures

Digital signatures are often used in the following situations:

- To provide a unique proof of data source
- To authenticate a user by using that person's private key, and the signature it generates
- To prove the authenticity and integrity of PKI certificates
- To provide a secure time stamp

The following steps indicate how digital signatures function:

Step 1. A user wants to sign some data. The user uses a signature algorithm with a personal signature key; only the signer knows this signature key.

Step 2. Based on the input data and a signature key, the signature algorithm generates its output, called a digital signature.

Step 3. The sending device attaches the digital signature to the message and sends the message to the receiver.

Step 4. The receiving device verifies the signature with the verification key, which is usually public.

 Please see page 88 for more details.

Step 5. The receiving device inputs the message, the digital signature, and the verification key into the verification algorithm, which checks the validity of the digital signature.

Step 6. If the check is successful, the document was not changed after signing, and the document was originated by the signer of the document.

Cisco products use digital signatures for entity-authentication, data-integrity, and data-authenticity purposes:

- IPsec gateways and clients use digital signatures to authenticate their Internet Key Exchange (IKE) sessions.
- Cisco SSL endpoints and the Cisco Adaptive Security Device Manager (ASDM) use digital signatures to prove the identity of the SSL server.
- Some of the service-provider-oriented voice management protocols use digital signatures to authenticate the involved parties.

Asymmetric Encryption

Here are the steps used in asymmetric encryption:

Step 1. User A acquires User B's public key.

Step 2. User A uses User B's public key to encrypt a message, which is often a symmetric key, using an agreed-upon algorithm.

Step 3. User A transmits the encrypted message.

Step 4. User B uses his private key to decrypt, and reveal, the message.

 Please see page 88 for more details.

RSA

The RSA keys are usually 512 to 2048 bits long. The RSA algorithm is based on the fact that each entity has two keys, a public key and a private key. The public key can be published, but the private key must be kept secret.

RSA is mainly used for two services:

- To ensure confidentiality of data by performing encryption
- To perform authentication of data, nonrepudiation of data, or both by generating digital signatures

Diffie-Hellman (DH)

The DH algorithm is the basis of most modern automatic key exchange methods. The IKE protocol in IPsec VPNs uses DH algorithms extensively.

PKI

Overview

A PKI provides a framework upon which you can base security services, such as encryption, authentication, and nonrepudiation. A PKI allows for very scalable solutions and is becoming an extremely important authentication solution for VPNs.

Two important PKI terms

- **Certificate authority (CA)**: The trusted third party that signs the public keys of entities in a PKI-based system.
- **Certificate**: A document that has been signed by the CA. This binds the name of the security entity with its public key.

 Please see page 88 for more details.

The CA may be a single entity, or there may be a complex hierarchy of CAs.

X.509 is a well-known standard that defines basic PKI formats. The standard has been widely used with many Internet applications, such as SSL and IPsec.

Simple Certificate Enrollment Protocol (SCEP) is a PKI communication protocol used for automated VPN PKI enrollment.

IPsec VPN Fundamentals

This section ensures that you understand the fundamentals of the modern IPSec VPN. Coverage includes critical topics such as the function of IPSec and IKE.

VPN overview

IPsec is the primary technology used in VPNs. It provides the following in the network:

- Cost savings
- Security
- Scalability
- Compatibility with broadband

There are two types:

- Site-to-site
- Remote-access

Many Cisco devices can work together to form the VPN, including routers, firewalls, and Adaptive Security Appliances.

 Please see page 88 for more details.

IPsec overview

IPsec has many advantages, including the following:

- Offers protection for any number of applications, running over any number of networks, using any number of media.
- Security is provided at the network layer; upper layers are unaffected.
- IPsec is extremely scalable.

IPsec features two main framework protocols, as shown in Figure 4-1:

- **AH**: Authentication Header is used only when confidentiality is not required; it provides authentication of the IPsec traffic only.
- **ESP**: Encapsulating Security Payload provides confidentiality and authentication.

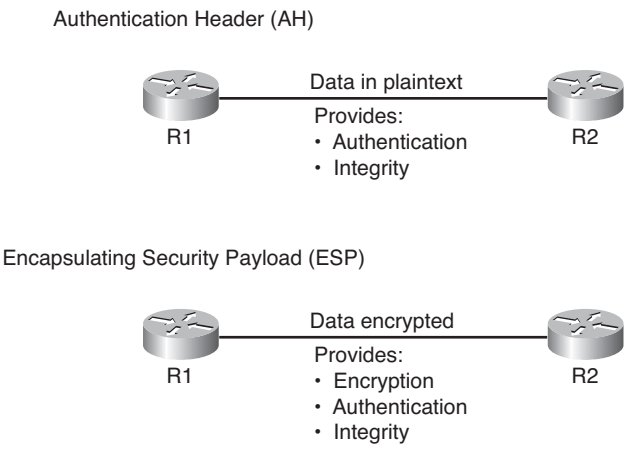


FIGURE 4-1
IPsec security protocols

You can apply ESP and AH to IP packets in two different modes:

- **Transport mode**: Security is provided only for the transport layer and above. Transport mode protects the payload of the packet but leaves the original IP address in the clear. ESP transport mode is used between two hosts that are both configured to support IPsec; these hosts handle the encryption/decryption process.
- **Tunnel mode**: Encapsulates the original IP header and creates a new IP header that is sent unencrypted across the untrusted network.

The following are some of the standard algorithms that IPsec uses:

- DES
- 3DES
- AES
- MD5
- SHA-1
- DH

IKE

IPsec uses the IKE protocol for the following:

- Negotiation of security association (SA) characteristics
- Automatic key generation
- Automatic key refresh
- Manageable manual configuration

 Please see page 88 for more details.

IKE uses three modes of operation:

- **Main mode**: An IKE session begins with one computer sending a proposal to another computer. The proposal sent by the initiator defines which encryption and authentication protocols are acceptable, how long keys should remain active, and whether perfect forward secrecy should be enforced.
- **Aggressive mode**: Compresses the IKE SA negotiation phases that are described thus far into three packets.
- **Quick mode**: Similar to aggressive mode IKE negotiation, except that negotiation is protected within an IKE SA.

IKE executes the following phases:

- **IKE Phase 1**: Two IPsec peers perform the initial negotiation of SAs. Phase 1 generates an Internet Security Association and Key Management Protocol (ISAKMP) SA, used for management traffic.
- **IKE Phase 2**: SAs are negotiated by the IKE process ISAKMP on behalf of other services, such as IPsec, that need encryption key material for operation. IKE Phase 2 is used to build IPsec SAs, which are for passing end-user data. Additional service negotiations occur in IKE Phase 1, DPD, Mode Config, and so on.

Site-to-Site VPN Construction

This section details the exact steps in creating the popular site-to-site VPN.

Operations

VPN negotiation occurs as follows:

1. An IPsec tunnel is initiated when Host A sends “interesting” traffic to Host B. Traffic is considered interesting when it travels between the IPsec peers and meets the criteria that is defined in the crypto ACL.

 Please see page 88 for more details.

2. In IKE Phase 1, the IPsec peers (Routers A and B) negotiate the established IKE SA policy. After the peers are authenticated, a secure tunnel is created using ISAKMP.
3. In IKE Phase 2, the IPsec peers use the authenticated and secure tunnel to negotiate IPsec SA transforms. The negotiation of the shared policy determines how the IPsec tunnel is established.
4. The IPsec tunnel is created, and data is transferred between the IPsec peers based on the IPsec parameters that are configured in the IPsec transform sets.
5. The IPsec tunnel terminates when the IPsec SAs are deleted or when their lifetime expires.

VPN configuration

To configure a site-to-site IPsec VPN, follow these steps:

Step 1. Ensure that existing access lists are compatible with IPsec; use **show access-lists**.

Step 2. Configure an ISAKMP policy to determine the ISAKMP parameters that will be used to establish the tunnel. Use the **crypto isakmp policy** command to define an IKE policy.

Step 3. Define the IPsec transform set. The definition of the transform set defines the parameters that the IPsec tunnel uses, and can include the encryption and integrity algorithms. Use the **crypto ipsec transform-set** global configuration command.

Step 4. Create a crypto ACL. The crypto ACL defines which traffic should be sent through the IPsec tunnel and be protected by the IPsec process.

Step 5. Create and apply a crypto map. The crypto map groups the previously configured parameters and defines the IPsec peer devices. The crypto map is applied to the outgoing interface of the VPN device. Use the **crypto map** global configuration command and interface configuration command.

 Please see page 88 for more details.

Step 6. Configure the interface ACL. Usually, there are restrictions on the interface that the VPN traffic uses (for example, block all traffic that is not IPsec or IKE).

Verification commands include **show crypto isakmp policy**, **show crypto ipsec transform-set**, and **show crypto map**.

VPN configuration with SDM

Choose **Configure > VPN** to open the VPN page.

The Cisco SDM VPN wizards use two sources to create a VPN connection:

- User input during a step-by-step wizard process
- Preconfigured VPN components

The Cisco SDM provides some default VPN components:

- Two IKE policies
- An IPsec transform set for the Quick Setup wizard

 Please see page 88 for more details.

Understanding Intrusion Prevention and Detection

Cisco provides intrusion detection and prevention in a variety of ways in its current security portfolio. You might add this powerful tool to your network via a dedicated hardware appliance known as a sensor, or you might add this functionality using a network module inserted into a router or a switch. However you decide to implement the technology, the goal is the same: to take some action based on an attack introduced to your network. This action might be to alert the network administrator via an automated notification, or it might be to prevent the attack from dropping the packet at a device.

Intrusion Prevention Versus Intrusion Detection

Intrusion detection is powerful in that you can be notified when potential problems or attacks are introduced into your network. Note, however, that detection cannot prevent these attacks from occurring. Detection cannot prevent the attacks because it operates on copies of packets. Often, these copies of packets are received from another Cisco device (typically a switch). Sensors operating using intrusion detection are said to be running in promiscuous mode.

Intrusion prevention is more powerful in that potential threats and attacks can be stopped from entering your network, or a particular network segment. Prevention is possible by the sensor because it is operating inline with packet flows.

IPS/IDS Terminology

You should be aware of many security terms that are related to intrusion detection and prevention technologies.

 Please see page 88 for more details.

Vulnerability

A vulnerability is a weakness that compromises the security or functionality of a particular system in your network. An example of a vulnerability is a web form on your public website that does not adequately filter inputs and guard against improper data entry. An attacker might enter invalid characters in an attempt to corrupt the underlying database.

Exploit

An exploit is a mechanism designed to take advantage of vulnerabilities that exist in your systems. For example, if you have poor passwords in use in your network, a password-cracking package might be the exploit aimed at this vulnerability.

False alarms

False alarms are IPS events that you do not want occurring in your implementation. There are two types of these alarms: false positive and false negative. Both are undesirable.

False positive

A false positive means that an alert has been triggered, but it was for traffic that does not constitute an actual attack. This type of traffic is often referred to as benign traffic.

False negative

A false negative occurs when attack traffic does not trigger an alert on the IPS device. This is often viewed as the worst type of false alarm, for obvious reasons.

 Please see page 88 for more details.

True alarms

There are two types of true alarms in IPS terminology. Both true positives and true negatives are desirable.

True positive

A true positive means that an attack was recognized and responded to by the IPS device.

True negative

This means that nonoffending or benign traffic did not trigger an alarm.

Promiscuous Versus Inline Mode

IDS/IPS sensors operate in promiscuous mode by default. This means that a device (often a switch) captures traffic for the sensor and forwards a copy for analysis to the sensor. Because the device is working with a copy of the traffic, the device is performing intrusion detection. It can detect an attack and send an alert (and take other actions), but it does not prevent the attack from entering the network or a network segment. It cannot prevent the attack, because it is not operating on traffic "inline" in the forwarding path. Figure 5-1 shows an example of a promiscuous mode IDS implementation.

If a Cisco IPS device is operating in inline mode, it can do prevention as opposed to mere detection. This is because the IPS device is in the actual traffic path. This makes the device more effective against worms and atomic attacks (attacks that are carried out by a single packet). Figure 5-2 shows an example of inline mode IPS.

FIGURE 5-1
Promiscuous mode (IDS)

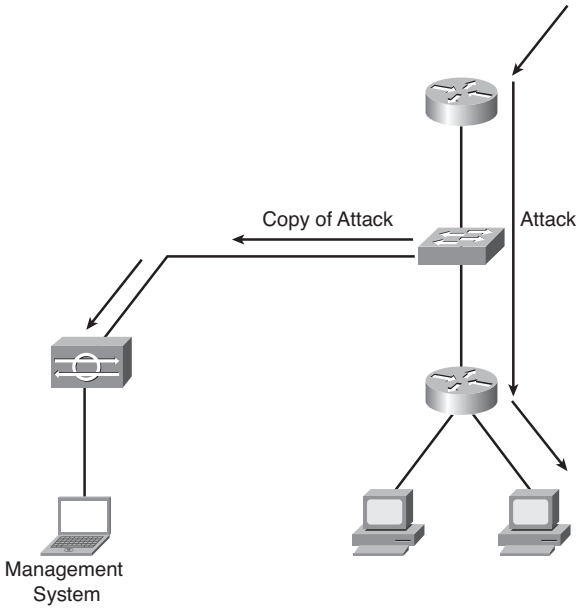
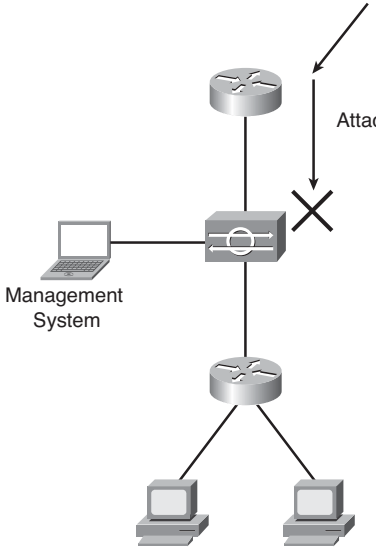


FIGURE 5-2
Inline mode (IPS)



To configure inline mode, you require two monitoring interfaces that are defined in the sensor as an inline pair. This pair of interfaces acts as a transparent Layer 2 structure that can to drop an attack that fires a signature.

Keep in mind that a sensor could be configured inline but could be set up so that it only alerts and doesn't drop packets. This is an example of an inline configuration in which only intrusion detection is performed.

Cisco Intrusion Prevention System (IPS) Version 6.0 software permits a device to do promiscuous mode and inline mode simultaneously. This allows one segment to be monitored for intrusion detection only, whereas another segment features intrusion prevention protection.

Approaches to Intrusion Prevention

A device can take many different approaches to securing the network using IPS. This section describes these various approaches.

Signature-based

Although Cisco uses a blend of detection and prevention technologies, signature-based IPS is the primary tool used by Cisco IPS solutions. Cisco releases signatures that are added to the device that identify a pattern that the most common attacks present. This is much less prone to false positives and ensures that IPS devices are stopping common threats. This type of approach is also known as pattern matching. As different types of attacks are created, these signatures can be added, tuned, and updated to deal with the new attacks.

Anomaly-based

This type of IPS technology is often called profile-based. It attempts to discover activity that deviates from what an engineer defines as "normal" activity. Because it can be so difficult to define what is normal activity for a given network, this approach tends to be prone to a high number of false positives.

 Please see page 88 for more details.

There are two common types of anomaly-based IPS: statistical anomaly detection and nonstatistical. The statistical approach learns about the traffic patterns on the network itself, and the nonstatistical method uses information coded by the vendor.

Policy-based

With this type of technology, the security policy is "written" into the IPS device. Alarms are triggered if activities are detected that violate the security policy coded by the organization. Notice how this differs from signature-based. Signature-based focuses on stopping common attacks, whereas policy-based is more concerned with enforcing the security policy of the organization.

Protoco-analysis-based

Although this approach is similar to signature based, it looks deeper into packets thanks to a protocol-based inspection of the packet payload that can occur. Most signatures examine rather common settings, but the protocol-analysis-based approach can do much deeper packet inspection and is more flexible in finding some types of attacks.

Exploring Evasive Techniques

Because attackers are aware of IPS technologies, they have developed ways to counter these devices in an attempt to continue attacks on network systems.

 Please see page 88 for more details.

String match

In this type of attack, strings in the data are changed in minor ways in an attempt to evade detection.

Obfuscation is one way in which control characters, hexadecimal representation, or Unicode representation help to disguise the attack. Another string match type of evasive technique is to just change the case of the string.

Fragmentation

With this evasive measure, the attacker breaks the attack packets into fragments so that they are more difficult to recognize. Fragmentation adds a layer of complexity for the sensor, which now must engage in the resource-intensive process of reassembling the packets.

Session

In this type of attack, the attacker spreads around the attack using a large number of very small packets, not using fragmentation in the approach. TCP segment reassembly can be used to combat this evasive measure.

Insertion

In this evasive technique, the attacker inserts data that is harmless along with the attack data. The IPS sensor does not fire an alert based on the harmless data. The end system ignores the harmless data and processes only the attack data.

Evasion

With this type of evasive technique, the attacker has the sensor see a different data stream than the intended victim. Unlike the insertion attack, the end system sees more data than the sensor, which results in an attack.

TTL-based

One way to implement an insertion attack is to manipulate the Time-to-Live value of fragments. With this evasive procedure, the IPS sensor sees a different data stream than the end system thanks to the manipulation of the TTL field in the IP header.

Encryption-based

This is an effective means of having attacks enter the network. The attacker sends the attack via an encrypted session. The encrypted attack cannot be detected by the IPS device. Because this method of foiling the IPS device exists, care must be taken to ensure that encrypted sessions cannot be established by attackers.

Resource exhaustion

Another evasive approach is to just overwhelm the sensor. Often, attackers simply try to overwhelm the physical device or the staff in charge of monitoring by flooding the device with alarm conditions.

Cisco Solutions and Products

Cisco offers many products and solutions that address your need for intrusion detection/prevention in your network infrastructure. This *CCNA Security Quick Reference* focuses on Cisco products that can run version 6.0 of the Cisco IPS Sensor Software. This 6.0 version adds many new features, including the following:

- **Virtualization support**: Allowing different policies for different segments that are being monitored by a single sensor.
- **New signature engines**: Additions to cover Server Message Block and Transparent Network Substrate traffic.

 Please see page 88 for more details.

- **Passive operating system fingerprinting**: A set of features that enables Cisco IPS to identify the OS of the victim of an attack.
- **Improved risk- and threat-rating system**: The risk rating helps with alerts and is now based on many different components to improve the performance and operation of the sensor.
- **External product interface**: Allows sensors to subscribe for events from other devices.
- **Enhanced password recovery**: Password recovery no longer requires reimaging.
- **Improved Cisco IPS Device Manager (IDM)**: New and improved GUI for management.
- **Anomaly detection**: Designed to detect worm-infested hosts.

Cisco Sensor family

The Cisco Sensor family includes the following devices:

- Cisco IOS IPS
- Cisco IDS Network Module
- Cisco IDS 4215 Sensor
- Cisco IDS 4240 Sensor
- Cisco ASA AIP-SSM
- Cisco IPS 4255 Sensor
- Cisco Catalyst 6500 Series IDSM-2
- Cisco IPS 4260 Sensor

 Please see page 88 for more details.

The following legacy devices can also run IPS 6.0 software:

- Cisco IDS 4235 Sensor
- Cisco IDS 4250 XL Sensor

Sensor Software Solutions

Many options are available for configuration and management of Cisco sensors. Also, the sensor operating systems and overall architecture is worth exploring for the certification exam and beyond.

IPS Sensor Software architecture

IPS Sensor Software Version 6.0 runs on the Linux OS. The components include the following:

- Event Store (provides storage for all events)
- SSH and Telnet (by default, Telnet is disabled)
- Intrusion Detection Application Programming Interface (IDAPI)
- MainApp
- SensorApp (for packet capture and analysis)
- Sensor interfaces

 Please see page 88 for more details.

Management options

For single-device (element) management, options include the following:

- Command-line interface (CLI)
- Cisco IDM (a graphical user interface)

For multiple-device management (enterprise management), options include the following:

- Cisco IPS Event Viewer
- Cisco Security Manager
- Cisco Security MARS (Cisco Security Monitoring, Analysis, and Response System)

Network IPS

Network IPS refers to the deployment of devices (typically sensors) in the network that capture and analyze traffic as it traverses the network. Because the sensor is analyzing network traffic, it can protect many hosts at the same time.

Host IPS

A host IPS solution features software installed on servers and workstations. Note that this solution does not require additional hardware (sensors). The Cisco host IPS is called Cisco Security Agent. It complements network IPS by protecting the integrity of applications and operating systems.

 Please see page 88 for more details.

Deploying Sensors

Technical factors to consider when selecting sensors for deployment in an organization include the following:

- The network media in use
- The performance of the sensor
- The overall network design
- The IPS design (Will the sensor analyze and protect many systems or just a few?)
- Virtualization (Will multiple virtual sensors be created in the sensor?)

Important issues to keep in mind in an IPS design include the following:

- **Your network topology**: Size and complexity, connections, and the amount and type of traffic.
- **Sensor placement**: It is recommended that these be placed at those entry and exit points that provide sufficient IPS coverage.
- **Your management and monitoring options**: The number of sensors often dictates the level of management you need.

Locations that generally need to be protected include the following:

- **Internet**: Sensor between your perimeter gateway and the Internet
- **Extranet**: Between your network and extranet connection
- **Internal**: Between internal data centers
- **Remote access**: Hardens perimeter control
- **Server farm**: Network IPS at the perimeter and host IPS on the servers

 Please see page 88 for more details.

Configuring Cisco IOS IPS Using Security Device Manager (SDM)

Cisco IOS IPS signatures include the following advanced features:

- Regular-expression string pattern matching
- Support for various response actions
- Alarm summarization
- Threshold configuration
- Anti-evasive techniques

To configure IPS using the SDM, choose **Configure > Intrusion Prevention**.

IPS signatures are loaded as part of the procedure to create a Cisco IOS IPS rule using the IPS Rule wizard. To view the configured Cisco IOS IPS signatures on the router, choose **Configure > Intrusion Prevention > Edit IPS > Signatures > All Categories**.

To view SDEE alarm messages in Cisco SDM, choose **Monitor > Logging > SDEE Message Log**.

To view alarms that are generated by Cisco IOS IPS, choose **Monitor > Logging > Syslog**.

 Please see page 88 for more details.

Endpoint Security

Securing endpoints in the network infrastructure is also very important. This section details the Cisco approach to this important security area.

Overview

The Cisco strategy for addressing host security is based on three broad elements:

- **Endpoint protection**: Cisco Security Agent protects endpoints against threats posed by viruses, Trojan horses, and worms.
- **Cisco Network Admission Control (NAC)**: Ensures that every endpoint complies with network security policies before being granted access to the network.
- **Network infection containment**: Containment focuses on automating key elements of the infection response process. Cisco NAC, Cisco Security Agent, and Intrusion Prevention System (IPS) provide this service.

The following techniques help protect an endpoint from operating system vulnerabilities:

- **Least-privilege concept**: A process should never be given more privilege than is necessary to perform a job.
- **Isolation between processes**: An operating system should provide isolation between processes; this prevents rogue applications from affecting the operating system or other application.
- **Reference monitor**: An access control concept that refers to a mechanism that mediates all access to operating system and application objects.
- **Small, verifiable pieces of code**: Small, easily verifiable pieces of software that are managed and monitored by a reference monitor.

 Please see page 88 for more details.

Buffer overflows

Buffer overflow exploits overwrite memory on an application stack by supplying too much data into an input buffer. Buffer overflows are used to "root" a system or to cause a DoS attack. "Rooting a system" is hacking a system so that the attacker has root privileges.

Worm attacks

A worm attack consists of the following:

- The enabling vulnerability
- A propagation mechanism
- The payload

The worm attack occurs in phases:

- **Probe phase**: Identifies vulnerable targets.
- **Penetrate phase**: Exploit code is transferred to the vulnerable target.
- **Persist phase**: The code tries to persist on the target system.
- **Propagate phase**: Extends the attack to other targets.
- **Paralyze phase**: Actual damage is done to the system.

IronPort

Cisco IronPort security appliances protect enterprises against Internet threats, with a focus on e-mail and web security products.

 Please see page 88 for more details.

The following are the security appliance products that IronPort offers:

- **IronPort C-Series**: E-mail security appliances
- **IronPort S-Series**: Web security appliance
- **IronPort M-Series**: Security management appliance

Cisco NAC

Cisco NAC products are designed to allow only authorized and compliant systems to access the network and to enforce network security policy. The Cisco NAC Appliance includes the following components:

- **Cisco NAC Appliance Server (NAS)**: Performs network access control
- **Cisco NAC Appliance Manager (NAM)**: Centralized administrative interface
- **Cisco NAC Appliance Agent (NAA)**: Client software that facilitates network admission
- **Rule-set updates**: Automatic updates

Cisco Security Agent

This product consists of the following:

- Management Center for Cisco Security Agents
- Cisco Security Agent

 Please see page 88 for more details.

Protection of end systems is provided by

- File system interceptor
- Network interceptor
- Configuration interceptor
- Execution space interceptor

Storage-Area Network Security

Storage-Area Networking is another topic that is becoming more and more important. This topic is explored in this section, with a special emphasis on security for SANs.

Overview

A storage-area network (SAN) is a specialized network that enables fast, reliable access among servers and external storage resources. Cisco solutions for intelligent SANs provide a better way to access, manage, and protect growing information resources across a consolidated Fibre Channel, Fibre Channel over IP (FCIP), Internet Small Computer Systems Interface (iSCSI), Gigabit Ethernet, and optical network.

Logical unit number masking

In computer storage, a logical unit number (LUN) is an address for an individual disk drive and the disk device itself. LUN masking is an authorization process that makes a LUN available to some hosts and unavailable to others.

 Please see page 88 for more details.

World Wide Names

A World Wide Name (WWN) is a 64-bit address that Fibre Channel networks use to uniquely identify each element in a Fibre Channel network. Zoning can use WWNs to assign security permissions. Zoning can also use name servers in the switches to either allow or block access to particular WWNs in the fabric.

Fibre Channel fabric zoning

Fibre Channel zoning is the partitioning of a Fibre Channel fabric into smaller subsets. If a SAN contains several storage devices, one device should not necessarily be allowed to interact with all the other devices in the SAN.

Virtual SAN

A virtual storage-area network (VSAN) is a collection of ports from a set of connected Fibre Channel switches that form a virtual fabric. You can partition ports within a single switch into multiple VSANs.

SAN security scope

SAN security should focus on six areas:

- SAN management access
- Fabric access
- Target access
- SAN protocol
- IP storage access
- Data integrity and secrecy

 Please see page 88 for more details.

Voice Security

Voice over IP is becoming more and more popular. This section details this technology and lists important related security topics.

Overview

The following components can be found in the VoIP network:

- **IP phones**
- **Call agents**: Replace many of the features previously provided by PBXs
- **Gateways**: Can forward calls between different types of networks
- **Gatekeepers**: Can be thought of as the "traffic cops" of the WAN
- **Multipoint control units (MCU)**: Useful for conference calling
- **Application servers**: Offer additional services such as voice mail
- **Videoconference stations**: Devices/software that allow a calling or called party to view/transmit video as part of their telephone conversation

Common VoIP protocols include the following:

- **H.323**: A suite of protocols that also defines certain devices, such as VoIP gateways and gatekeepers.
- **MGCP**: Originally developed by Cisco, Media Gateway Control Protocol enables a client (for example, an analog port in a voice-enabled router) to communicate with a server (for example, a Cisco Unified Communications server) via a series of events and signals.

 Please see page 88 for more details.

- **H.248**: H.248 is similar to MGCP, but it is more flexible in its support for gateways and applications. It defines the necessary control mechanism to allow a media gateway controller to control gateways to support multimedia streams across networks.
- **SIP**: Session Initiation Protocol is a very popular protocol to use in mixed-vendor environments.
- **SCCP**: Skinny Client Control Protocol is a Cisco-proprietary signaling protocol.
- **RTP**: Real-time Transport Protocol carries the voice payload.
- **RTCP**: RTP Control Protocol provides information about an RTP flow.
- **SRTP**: Secure RTP secures the RTP traffic.

Common voice security issues

Common attacks include the following:

- Accessing VoIP resources without proper credentials
- Gleaning information from unsecured networks
- Launching a denial-of-service attack
- Capturing telephone conversations
- VoIP spam (more commonly referred to as spam over IP telephony, or SPIT)
- Vishing (similar to phishing, but refers to maliciously collecting such information over the phone)
- SIP attacks (man-in-the-middle attacks and manipulation of SIP messages)

 Please see page 88 for more details.

Protection mechanisms

Mechanisms and methods to help secure the VoIP network include the following:

- Auxiliary VLANs (with voice traffic getting its own VLAN).
- Security appliances.
- Use IPsec protected VPNs.
- Disable web access.
- Disable gratuitous ARP.
- Disable unneeded services.

Mitigating Layer 2 Attacks

Later 2 is often omitted from security practices, but it should not be. This section details many important security practices that should be followed.

VLAN hopping

Attackers can send traffic into another VLAN by double-tagging 802.1Q information in the frame and using the native VLAN. One easy way to combat this is to create an empty VLAN for the native VLAN and then use this as the native VLAN on all links. Also, ensure that switch ports are not using Dynamic Trunking Protocol (DTP) by using the **switchport nonegotiate** command.

 Please see page 88 for more details.

STP protections

Consider the following protection mechanisms:

- **BPDU Guard**: Ensures that bridges plugged into PortFast ports do not cause a temporary Layer 2 loop.
- **Root Guard**: Denies a new root switch from being elected in the topology from an unauthorized port.

Port security

Use this feature to lock down a port for authorized MAC address usage. To enable the feature and configure options, use the command **switchport port-security**. Figure 6-1 shows an example of port security configurations.

FIGURE 6-1
Port security

```
Switch1(config)# switchport port-security
Switch1(config)# switchport port-security maximum 2
Switch1(config)# switchport port-security violation restrict
Switch1(config)# switchport port-security aging time 120
```

Additional security features

- **Switched Port Analyzer (SPAN) and Remote SPAN (RSPAN)**: Used to copy frames to a destination port for analysis
- **Storm control**: Used to prevent an excess of unicast, broadcast, or multicast frames in the LAN
- **MAC address notifications**: Alerts when the MAC address on a port changes

 Please see page 88 for more details.

Layer 2 best practices

Best practices include the following:

- Manage switches securely.
- Use a dedicated VLAN for trunks.
- Do not use VLAN 1.
- Set user ports to nontrunking.
- Use port security.
- Selectively use Simple Network Management Protocol (SNMP).
- Enable STP security features.
- Trim Cisco Discovery Protocol (CDP).
- Disable unused ports, and place them in a VLAN.

 Please see page 88 for more details.

CCNA Security Quick Reference

Anthony Sequeira

Published by:
Cisco Press
800 East 96th Street
Indianapolis, Indiana 46240 USA

First Release June 2008

ISBN-13: 978-1-58705-766-3

ISBN-10: 1-58705-766-2

Warning and Disclaimer

This digital Short Cut is designed to provide information about the CCNA Security Certification. Every effort has been made to make this digital Short Cut as complete and accurate as possible, but no warranty or fitness is implied.

The information is provided on an "as is" basis. The author, Cisco Press, and Cisco Systems, Inc. shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this digital Short Cut.

The opinions expressed in this digital Short Cut belong to the author and are not necessarily those of Cisco Systems, Inc.

Trademark Acknowledgments

All terms mentioned in this digital Short Cut that are known to be trademarks or service marks have been appropriately capitalized. Cisco Press or Cisco Systems, Inc. cannot attest to the accuracy of this information. Use of a term in this digital Short Cut should not be regarded as affecting the validity of any trademark or service mark.

Feedback Information

At Cisco Press, our goal is to create in-depth technical books of the highest quality and value. Each book is crafted with care and precision, undergoing rigorous development that involves the unique expertise of members of the professional technical community.

Reader feedback is a natural continuation of this process. If you have any comments on how we could improve the quality of this digital Short Cut, or otherwise alter it to better suit your needs, you can contact us through e-mail at feedback@ciscopress.com. Please be sure to include the digital Short Cut title and ISBN in your message.

We greatly appreciate your assistance.

Corporate and Government Sales

The publisher offers excellent discounts on this digital Short Cut when ordered in quantity for bulk purchases or special sales, which may include electronic versions and/or custom covers and content particular to your business, training goals, marketing focus, and branding interests. For more information, please contact: **U.S. Corporate and Government Sales** 1-800-382-3419 corpsales@pearsontechgroup.com.

For sales outside the United States please contact: **International Sales** international@pearsoned.com

Americas 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: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.