Exam Topics in This Chapter

- Remote Authentication Dial-In User Service (RADIUS)
- Terminal Access Controller Access Control System Plus (TACACS+)
- Advanced Encryption Standard (AES)
- EAP, PEAP, TKIP, TLS
- Data Encryption Standard (DES)
- Triple DES (3DES)
- IP Security (IPSec)
- Internet Key Exchange (IKE)
- Certificate Enrollment Protocol (CEP)
- Point-to-Point Tunneling Protocol (PPTP)
- Layer 2 Tunneling Protocol (L2TP)

You can find a list of all of the exam topics in the introduction to this book. For the latest updates on exam topics, visit Cisco.com.

CHAPTER 4

Security Protocols

This chapter covers some of today's most widely used technologies that enable network administrators to ensure that sensitive data is secure from unauthorized sources.

Standards such as IP Security (IPSec) and encryption standards are covered, as are all the fundamental foundation topics you need to understand to master the topics covered in the CCIE Security written exam.

The chapter ends with a discussion of some of the security features used in wireless networking to improve security. Protocols such as Extensible Authentication Protocol (EAP), Protected Extensible Authentication Protocol (PEAP), Temporal Key Integrity Protocol (TKIP), Message Integrity Check (MIC), and Transport Layer Security (TLS) are discussed, all of which are newly defined protocols used to help secure vulnerable wireless networks.

This chapter covers the following topics:

- **Security protocol topics**—Sections are included for authentication, authorization, and accounting (AAA), RADIUS, and TACACS+.
- **Encryption Technology Overview**—Covers encrypting IP using standard encryption such as 3DES, AES, and IPSec. The mechanism used to authenticate encryption tunnels is also covered.
- **Certificate Enrollment Protocol**—Describes the Cisco-defined certificate management protocol, CEP, and how a device communicates with a Certificate Authority (CA).
- **EAP, PEAP, and TKIP**—Shows common new mechanisms used in the fight to keep intruders and hackers away from wireless networks.

"Do I Know This Already?" Quiz

The purpose of this assessment quiz is to help you determine how to spend your limited study time.

If you can answer most or all of these questions, you might want to skim the "Foundation Topics" section and return to it later, as necessary. Review the "Foundation Summary" section and answer the questions at the end of the chapter to ensure that you have a strong grasp of the material covered.

If you already intend to read the entire chapter, you do not necessarily need to answer these questions now. If you find these assessment questions difficult, read through the entire "Foundation Topics" section and review it until you feel comfortable with your ability to answer all of these questions and the "Q & A" questions at the end of the chapter.

Answers to these questions can be found in Appendix A, "Answers to Quiz Questions."

1. What are the three components of AAA? (Choose the three best answers.)
   a. Accounting
   b. Authorization
   c. Adapting
   d. Authentication
2. What Cisco IOS command must be issued to start AAA on a Cisco router?
   a. aaa old-model
   b. aaa model
   c. aaa new model
   d. aaa new-model
   e. aaa new_model
3. What mathematical algorithm initiates an encrypted session between two routers by exchanging public keys over an insecure medium such as the Internet?
   a. Routing algorithm
   b. Diffie-Hellman algorithm
   c. The switching engine
   d. The stac compression algorithm
4. Can you configure RADIUS and TACACS+ to be used on the same router?
   a. No.
   b. Yes, provided you have the same lists names applied to the same interfaces.
   c. Yes, provided you have the different lists names applied to the same interfaces.
   d. Yes, provided you have the different list names applied to different interfaces.

5. How do you remotely launch ACS to a Windows 2000 device? (The remote IP address is 10.1.1.1 and the client is Internet Explorer.)

   a. Type launch.
   b. Type 10.1.1.1.
   c. Type 10.1.1.1:2002.
   d. Type 10.1.1.1:8080.

6. What RADIUS attribute is used by vendors and not predefined by RFC 2138?

   a. 1
   b. 2
   c. 3
   d. 4
   e. 13
   f. 26
   g. 333
   h. 33

7. RADIUS can support which of the following protocols?

   a. PPP
   b. OSPF
   c. AppleTalk
   d. IPX
   e. NLSP

8. When a RADIUS server identifies the wrong password entered by the remote user, what packet type is sent?

   a. ACCEPT-USER
   b. REJECT-USERS
   c. REJECT-DENY
   d. REJECT-ACCEPT
   e. REJECT-ERROR
   f. ACCESS-REJECT

9. Identify the false statement about RADIUS.

   a. RADIUS is a defined standard in RFC 2138/2139.
   b. RADIUS runs over TCP port 1812.
   c. RADIUS runs over UDP port 1812.
   d. RADIUS accounting information runs over port 1646.

10. What is the RADIUS key for the following configuration? If this configuration is not valid, why isn't it? (Assume that this configuration is pasted into Notepad and not on an active router.)

```
aaa authentication login use-radius group radius local
aaa authentication ppp user-radius if-needed group radius
aaa authorization exec default group radius
aaa authorization network default group radius
radius-server 3.3.3.3
radius-server key IlovemyMum
```

    a. The RADIUS key is IlovemyMum, and it is a valid configuration.

    b. The RADIUS key is Ilovemymum, and it is a valid configuration.

    c. This configuration will not work because the command **aaa new-model** is missing**.**

    d. The RADIUS key is 3.3.3.3, and it is a valid configuration.

11. What is the RADIUS key for the following configuration?

```
aaa new-model
aaa authentication login use-radius group radius local
aaa authentication ppp user-radius if-needed group radius
aaa authorization exec default group radius
aaa authorization network default group radius
radius-server 3.3.3.3
radius-server key IlovemyMum
```

    a. The RADIUS key is IlovemyMum.

    b. The RADIUS key is Ilovemymum.

    c. No RADIUS key exists.

    d. The RADIUS key is 3.3.3.3.

12. What versions of TACACS does Cisco IOS support? (Select the best three answers.)

    a. TACACS+

    b. TACACS

    c. Extended TACACS

    d. Extended TACACS+

13. TACACS+ is transported over which TCP port number?

    a. 520

    b. 23

    c. 21

    d. 20

    e. 49

14. What is the predefined RADIUS server key for the following configuration?

```
radius-server host 3.3.3.3
radius-server key CCIEsrock
```

a. 3.3.3.3

b. Not enough data

c. CCIESROCK

d. CCIEsRock

e. CCIEsrock

15. What does the following command accomplish?

```
tacacs_server host 3.3.3.3
```

a. Defines the remote TACACS+ server as 3.3.3.3

b. Defines the remote RADIUS server as 3.3.3.3

c. Nothing, because it is not a valid IOS command

d. Configures a Radius server 3.3.3.3

e. An Invalid IOS command

16. Which of the following protocols does TACACS+ support?

a. PPP

b. AppleTalk

c. NetBIOS

d. All of these

17. Which of the following key lengths are *not* supported by AES?

a. 64

b. 128

c. 192

d. 256

e. 512

18. What is the number of bits used with a standard DES encryption key?

a. 56 bits

b. 32 bits; same as IP address

c. 128 bits

d. 256 bits

e. 65,535 bits

f. 168 bits

19. What is the number of bits used with a 3DES encryption key?
    a. 56 bits
    b. 32 bits; same as IP address
    c. 128 bits
    d. 256 bits
    e. 65,535 bits
    f. 168 bits
20. In IPSec, what encapsulation protocol encrypts only the data and not the IP header?
    a. ESP
    b. AH
    c. MD5
    d. HASH
21. In IPSec, what encapsulation protocol encrypts the entire IP packet?
    a. ESH
    b. ESP
    c. AH
    d. MD5
    e. HASH
22. Which of the following is AH's IP number?
    a. 23
    b. 21
    c. 50
    d. 51
    e. 500
    f. 444
23. Which of the following is ESP's IP number?
    a. 23
    b. 21
    c. 50
    d. 51
    e. 500
    f. 444

24. Which of the following is *not* part of IKE phase I negotiations?

- **a.** Authenticating IPSec peers
- **b.** Exchanging keys
- **c.** Establishing IKE security
- **d.** Negotiating SA parameters

25. Which of the following is *not* part of IKE phase II?

- **a.** Negotiating IPSec SA parameters
- **b.** Periodically updating IPSec SAs
- **c.** Occasionally updating SAs (at most, once a day)
- **d.** Establishing IPSec security parameters

26. Which is the fastest mode in IPSec?

- **a.** Main mode
- **b.** Fast mode
- **c.** Aggressive mode
- **d.** Quick mode

27. Certificate Enrollment Protocol (CEP) runs over what TCP port number? (Choose the best two answers.)

- **a.** Same as HTTP
- **b.** Port 80
- **c.** Port 50
- **d.** Port 51
- **e.** Port 333
- **f.** Port 444

28. Which of the following are new features aimed at increasing wireless security? (Choose the best four answers.)

- **a.** TKIP
- **b.** AES
- **c.** EAP
- **d.** PEAP
- **e.** MIC
- **f.** 802.1D
- **g.** ESP
- **h.** AH

Foundation Topics

Authentication, Authorization, and Accounting

Authentication, authorization, and accounting (AAA, pronounced triple A) provides security to Cisco IOS routers and network devices beyond the simple user authentication available on IOS devices.

AAA provides a method to identify which users are logged into a router and each user's authority level. AAA also provides the capability to monitor user activity and provide accounting information.

In today's IP networks, access to network data is available in a variety of methods, including the following:

- PSTN dialup modems
- ISDN dialup
- Internet access through virtual private networks (VPNs)

The AAA model is defined as follows:

- **Authentication**—Who are you?
- **Authorization**—What resources are you permitted to use?
- **Accounting**—What resources were accessed, at what time, by whom, and what commands were issued?

The three phases ensure that legitimate users are permitted access. A remote user must be authenticated before being permitted access to network resources.

Authentication allows the user to submit a username and password and permits challenges and responses. After the user is authenticated, authorization defines what services or resources in the network users are permitted access to. The operations permitted here can include IOS-privileged EXEC commands. For example, a user might type commands but be permitted to use only certain **show** and **debug** commands for which the user is authorized.

Accounting allows the network administrator to log and view what was actually performed (for example, if a Cisco router was reloaded or the configuration was changed). Accounting ensures

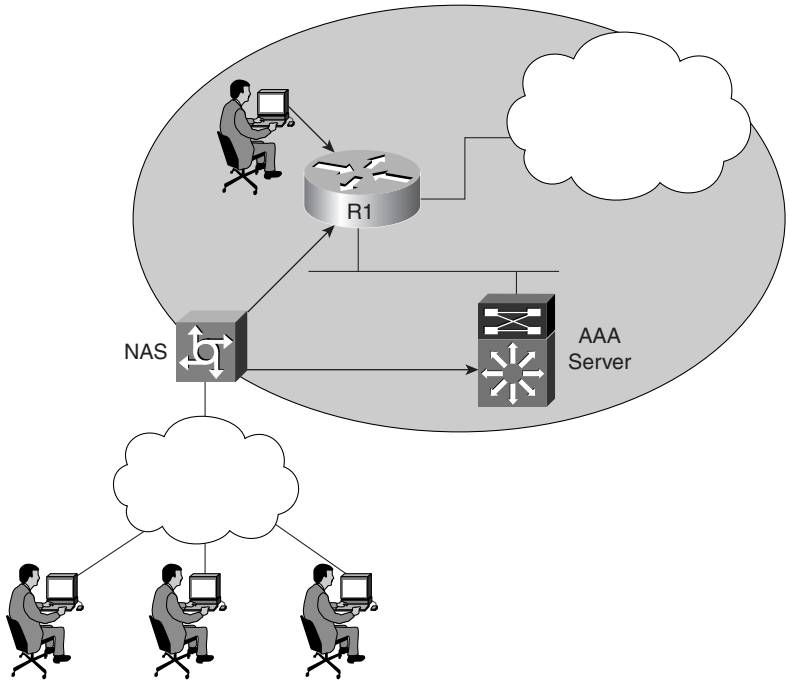
that an audit will enable network administrators to view what was performed and at what time it was performed. Accounting keeps track of the information needed to audit and report network resource usage. This typically includes the username, the start and stop time of login, and the commands typed by the user.

NOTE To start AAA on a Cisco router, issue the following IOS command:

```
aaa new-model
```

Figure 4-1 displays a typical secure network scenario.

Figure 4-1 *Secure Network Access*



The users could be dialup users running async (in this case, PSTN) or using ISDN with Point-to-Point Protocol (PPP). The network access server (NAS) ensures that only authenticated users have access to the secure network; it maintains resources and accounting information.

Authorization tells which resources, or host devices, are authorized to be accessed (such as FTP servers). The NAS implements the AAA protocols and also collects data regarding what network resources were accessed. The NAS can also ensure that devices in the secured network require authentication. For example, the users in Figure 4-1 who are accessing Router R1 require a valid username/password pairing to enter any IOS commands.

The following sections further define what authentication, authorization, and accounting are by discussing a common Cisco IOS router example.

Authentication

Authentication allows administrators to identify who can connect to a router by including the user's username and password. Normally, when a user connects to a router remotely by Telnet, the user must supply only a password, and the administrator has no way of knowing the user's username. You can, however, configure local usernames and passwords on a Cisco IOS router, but this does not scale well and it is not very secure. Configuring a small set of routers with individual usernames and passwords (IOS syntax **username** *username* **password** *password*) is fine, but doing so for large networks would be a difficult exercise to manage. Centrally locating the usernames and passwords is a better solution because only a few devices need to be updated and maintained. Also, users are not logged, and their configuration changes are not monitored without further configuration changes made on each individual router.

Example 4-1 displays a sample code snippet of a remote user accessing a AAA-configured Cisco router by Telnet.

Example 4-1 *Username/Password Pair Entry*

```
Sydney>telnet San-Fran
Trying san-fran (10.99.1.1)... Open User Access Verification
Username: drewrocks
Password: xxxxxxxx
San-Fran>
```

As you can see in Example 4-1, the user must enter a valid username and password to gain access to the router. Typically, a database containing the valid usernames resides locally on the router or on a remote security server.

Authorization

Authorization comes into play after authentication. Authorization allows administrators to control the level of access users have after they successfully gain access to the router. Cisco IOS allows certain access levels (called *privilege levels*) that control which IOS commands the user can issue. For example, a user with a privilege level of 0 cannot issue many IOS commands. There are five commands at privilege level 0: **disable**, **enable**, **exit**, **help**, and **logout**. A user with a privilege level of 15 can perform all valid IOS commands. The local database or remote security server can grant the required privilege levels.

Remote security servers, such as RADIUS and TACACS+, authorize users for specific rights by associating attribute-value (AV) pairs, which define those rights with the appropriate user. AAA

authorization assembles a set of attributes that describes what the user is authorized to perform. These attributes are compared with the information contained in a database for a given user, and the result is returned to AAA to determine the user's actual permissions and restrictions.

NOTE You can display the user's privilege level on a Cisco router with the **show privilege** command. The following code displays the privilege level when the enable password has already been entered:

```
R1#show privilege
Current privilege level is 15
```

The higher the privilege, the more capabilities a user has with the IOS command set.

Accounting

Accounting occurs after authentication and authorization have been completed. Accounting allows administrators to collect information about users. Specifically, administrators can track which user logged into which router, which IOS commands a user issued, and how many bytes were transferred during a user's session. For example, accounting enables administrators to monitor which routers have had their configurations changed. Accounting information can be collected by a remote security server.

To display local account information on a Cisco router collecting accounting information, issue the **show accounting** IOS command. Example 4-2 displays sample output when the command is issued on Router R1. (Note that for Cisco IOS 12.2T and higher, the command has changed to **show aaa user all**.)

Example 4-2 show accounting Command

```
R1#show accounting
Active Accounted actions on Interface Serial0:1, User jdoe Priv 1
 Task ID 15, Network Accounting record, 00:00:18 Elapsed
 task_id=15 timezone=PDT service=ppp mlp-links-max=4 mlp-links-current=4
protocol=ip addr=119.0.0.2 mlp-sess-id=1
      Overall Accounting Traffic
          Starts   Stops  Updates  Active  Drops
Exec           0       0        0       0       0
Network        8       4        0       4       0
Connect        0       0        0       0       0
Command        0       0        0       0       0
Rsrc-mgmt      1       0        0       1       0
System         0       0        0       0       0
 User creates:21, frees:9, Acctinfo mallocs:15, frees:6
Users freed with accounting unaccounted for:0
Queue length:0
```

Table 4-1 describes the fields contained in Example 4-2.

Table 4-1 **show accounting** *Fields*

Field	Description
User	The user's ID
Priv	The user's privilege level (0–15)
Task ID	Each accounting session's unique identifier
Accounting Record	Type of accounting session
Elapsed	Length of time (hh:mm:ss) for this session type

Rather than maintain a separate database with usernames, passwords, and privilege levels, you can use external security servers to run external security protocols—namely RADIUS and TACACS.

These security server protocols stop unauthorized access to your network. The following sections review these two security protocols.

Security Server Protocols

In many circumstances, AAA uses security protocols to administer its security functions. If your router or access server is acting as an NAS, AAA is the means through which you establish communication between your NAS and your RADIUS, TACACS+, or Kerberos security server.

Remote Authentication Dial-In User Service

RADIUS is a client/server-based system that secures a Cisco network against intruders. Implemented in Cisco IOS, RADIUS sends authentication requests to a RADIUS server. RADIUS was created by Livingston Enterprises and is now defined in RFCs 2865/2866 (RFCs 2138/2139 are now obsolete).

A RADIUS server is a device that has the RADIUS daemon or application installed. RADIUS must be used with AAA to enable the authentication, authorization, and accounting of remote users when using Cisco IOS routers.

When a RADIUS server authenticates a user, the following events occur:

1. The user is prompted for and enters a username and password.
2. The username and encrypted password are sent over the network to the RADIUS server. These events are sent via the packet format known as Access-Request.

3. The user receives one of the following responses from the RADIUS server:

   ACCESS-ACCEPT—The user is authenticated.

   ACCESS-REJECT—The user is not authenticated and is prompted to re-enter the username and password, or access is denied. The RADIUS server sends this response when the user enters an invalid username/password pairing.

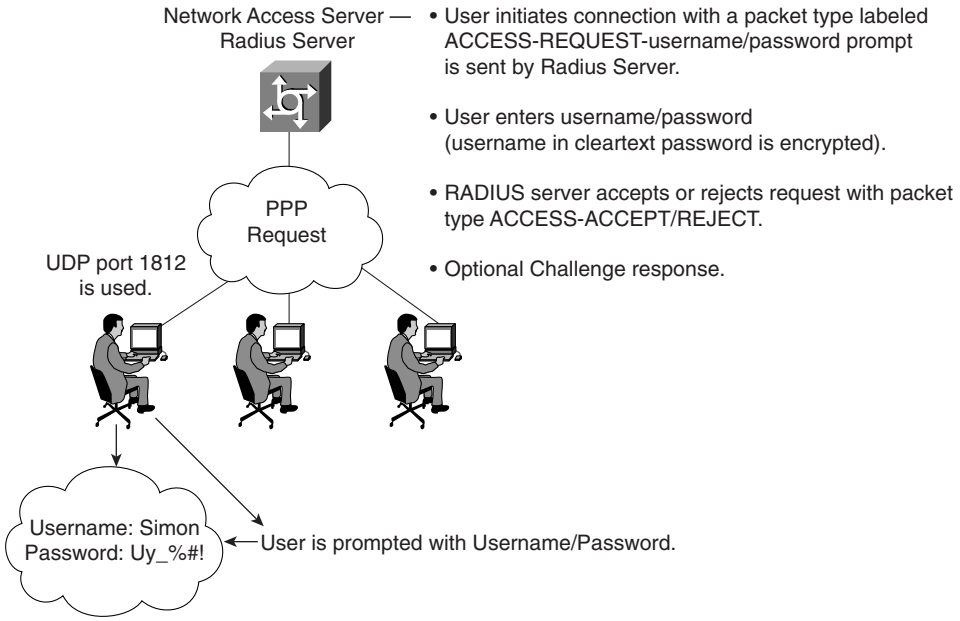
   ACCESS-CHALLENGE—A challenge is issued by the RADIUS server. The challenge collects additional data from the user.

   CHANGE PASSWORD—The RADIUS server issues a request asking the user to select a new password.

An ACCESS-ACCEPT or ACCESS-REJECT response may contain additional information for services that the user can access, including Telnet, rlogin, or local-area transport (LAT) connections, and PPP, Serial Line Internet Protocol (SLIP), or EXEC services.

RADIUS is commonly used when PPP is used. Figure 4-2 displays a typical PPP connection request to a RADIUS server.

Figure 4-2 *RADIUS Sequence Example*



The RADIUS server accepts or rejects a username and password pair. In some instances, a user might be asked to enter more information (this is called a challenge response). For example, if a user's password has expired, a RADIUS server prompts the user for a new password.

Transactions between the client (end user) and the RADIUS server are authenticated through a shared secret. The username is sent as clear text. RADIUS supports both Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP). PAP and CHAP are security protocols that allow users to gain access to remote devices with PPP. A RADIUS server will never send the user's password over the network in any circumstance. If the username/password pairing is entered incorrectly, the RADIUS server sends an ACCESS-REJECT response. The end user must re-enter the pairings or the connection will be rejected. Note that PAP sends the end user's password in the clear to the NAS, but from the NAS to the RADIUS server (the NAS and the RADIUS communicate using the shared secret), the end user's password is encrypted.

RADIUS supports a number of predefined attributes that can be exchanged between client and server, such as the client's IP address. RADIUS attributes carry specific details about authentication.

RFC 2138 defines a number of attributes. The following list provides details for the most common attributes:

- **Attribute type 1**—Username (defines usernames, such as numeric, simple ASCII characters, or a Simple Mail Transfer Protocol [SMTP] address).
- **Attribute type 2**—User Password (defines the password, which is encrypted using Message Digest 5 [MD5]).
- **Attribute type 3**—CHAP Password (used only in access-request packets).
- **Attribute type 4**—NAS IP Address (defines the NAS's IP address; used only in access-request packets).
- **Attribute type 5**—NAS Port (this is not the User Datagram Protocol [UDP] port number; it indicates the NAS's physical port number, ranging from 0 to 65,535).
- **Attribute type 6**—Service-Type of service requested or type of service to be provided. Now supported in Cisco IOS. See (requires CCO login) http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps1839/products_feature_guide09186a0080110bed.html#1024276.
- **Attribute type 7**—Framed-Protocol defines required framing; for example, PPP is defined when this attribute is set to 1 and SLIP is set to 2.
- **Attribute type 8**—Framed-IP-Address defines the IP address to be used by the remote user.
- **Attribute type 9**—Framed-IP-Netmask defines the subnet mask to be used by the remote user.
- **Attribute type 10**—Framed-Routing.

- **Attribute type 13**—Framed-Compression.
- **Attribute type 19**—Callback-Number.
- **Attribute type 26**—Vendor-Specific. Cisco (vendor-ID 9) uses one defined option: vendor type 1 named cisco-avpair; this attribute transmits TACACS+ A/V pairs.
- **Attribute type 61**—NAS-Port-Type

Table 4-2 summarizes the RADIUS protocol's main features.

Table 4-2 *Summary of RADIUS Protocol Features*

Feature	Description
UDP	Packets sent between the client and server are UDP, primarily because TCP's overhead does not allow for significant advantages. Typically, the user can wait for a username/password prompt.
UDP destination port	1812 and 1813. Defined in RFC 2865, which supersedes RFC 2138. Early deployments RADIUS used UDP ports 1645 and 1646.
Attributes	Attributes are used to exchange information between the NAS and client.
Model	Client/server-based model in which packets are exchanged in a unidirectional manner.
Encryption method	The password is encrypted using MD5; the username is not encrypted. RADIUS encrypts only the password in the access-request packet, sent from the client to the server. The remainder of the packet is transmitted in clear text. A third party could capture other information, such as the username, authorized services, and accounting information.
Multiprotocol support	Does not support protocols such as AppleTalk, NetBIOS, or IPX. IP is the only protocol supported.

Now, examine the RADIUS configuration tasks required on a Cisco router.

IETF Attribute 26 (Vendor-Specific) encapsulates vendor-specific attributes, thereby allowing vendors to support their own extended attributes. Attribute 26 contains the following three elements:

- Type
- Length
- String (also known as data)

RADIUS Configuration Task List

A RADIUS server is usually software that runs on a variety of platforms, including Microsoft Windows 2000 Server and various UNIX hosts. RADIUS can authenticate router users and even validate IP routes.

To configure RADIUS on your Cisco router or NAS, perform the following tasks:

Step 1 Enable AAA with the **aaa new-model** global configuration command. AAA must be configured if you plan to use RADIUS.

Step 2 Use the **aaa authentication** global configuration command to define method lists for RADIUS authentication.

Step 3 Use **line** and **interface** commands to enable the defined method lists to be used.

Step 4 Define the RADIUS server and secret key with the following IOS commands:

```
radius-server ip-address
radius-server key secret-key
```

> **NOTE** There are two optional RADIUS commands:
>
> Use the **aaa authorization** global command to authorize specific user functions.
>
> Use the **aaa accounting** command to enable accounting for RADIUS connections.

Examples are the best method to show the enormous IOS command set that is available for use when configuring RADIUS support with AAA.

Example 4-3 configures a Cisco IOS router with AAA and RADIUS support.

Example 4-3 *AAA and RADIUS IOS Configuration*

```
aaa new-model
aaa authentication login use-radius group radius local
aaa authentication ppp user-radius if-needed group radius
aaa authorization exec default group radius
aaa authorization network default group radius
radius-server 3.3.3.3
radius-server key ccie2005
! Ensure you apply the named access list on the VTY line
line vty 0 4
aaa authentication login
```

The command lines in this RADIUS authentication and authorization configuration are defined as follows:

- The **aaa authentication login use-radius group radius local** command configures the router to use RADIUS for authentication at the login prompt. If RADIUS returns an error, the user is authenticated using the local database. In this example, **use-radius** is the name of the method list, which specifies RADIUS and then local authentication. If the RADIUS server returns the ACCESS-REJECT response, the user is denied access and the router will not check its local database.
- The **aaa authentication ppp user-radius if-needed group radius** command configures the Cisco IOS software to use RADIUS authentication for lines using PPP with CHAP or PAP, if the user is not already authorized. If the EXEC facility has authenticated the user, RADIUS authentication is not performed. In this example, **user-radius** is the name of the method list defining RADIUS as the if-needed authentication method.
- The **aaa authorization exec default group radius** command sets the RADIUS information used for EXEC authorization, autocommands, and access lists.
- The **aaa authorization network default group radius** command sets RADIUS for network authorization, address assignment, and access lists.
- The **radius-server** commands define the NAS.
- The **radius-server key** commands define the shared secret text string between the NAS and the RADIUS server host.

Example 4-4 displays an example in which AAA is enabled on a Cisco IOS router.

Example 4-4 *AAA and RADIUS Example*

```
Hostname R1
username simon password SimonisisAgreatdrummeR
aaa new-model
aaa authentication ppp dialins group radius local
aaa authorization network default group radius local
aaa accounting network default start-stop group radius
aaa authentication login simon local
aaa authorization exec default local
radius-server host 3.3.3.3
radius-server key CCIEsrock
line vty 0 4
login authentication radius-login
```

The Example 4-4 line configurations are defined as follows:

- The **radius-server host** command defines the RADIUS server host's IP address.
- The **radius-server key** command defines the shared secret text string between the NAS and the RADIUS server host.
- The **aaa authentication ppp dialins group radius local** command defines the authentication method list, dialins, which specifies that RADIUS authentication and then (if the RADIUS server does not respond) local authentication will be used on serial lines using PPP.
- The **aaa authorization network default group radius local** command sets RADIUS for network authorization, address assignment, and access lists.
- The **aaa accounting network default start-stop group radius** command tracks PPP usage. This command is used for all network services. It can be PPP, but also SLIP or ARAP.
- The **aaa authentication login simon local** command defines the method list, simon, for local authentication.
- The **aaa authentication login simon** command applies the simon method list for login authentication.

NOTE A method list simply defines the authentication methods to be used, in sequence, to authenticate a user. Method lists enable you to designate one or more security protocols to be used for authentication, ensuring a backup system for authentication in case the initial method fails. Cisco IOS software uses the first method listed to authenticate users; if that method does not respond, the Cisco IOS software selects the next authentication method listed. This process continues until there is successful communication with a listed authentication method or the authentication method list is exhausted, in which case authentication fails.

TIP Cisco.com provides a long list of configuration examples. To view more detailed configurations, visit the following web address and follow the link to Security Management:
http://www.cisco.com/pcgi-bin/Support/browse/index.pl?i=Products&f=753&viewall=true

Terminal Access Controller Access Control System Plus

Cisco IOS supports three versions of TACACS—TACACS, extended TACACS, and TACACS+. All three methods authenticate users and deny access to users who do not have a valid username/password pairing. TACACS+ is Cisco proprietary, whereas RADIUS is an open standard originally created by Livingston Enterprises.

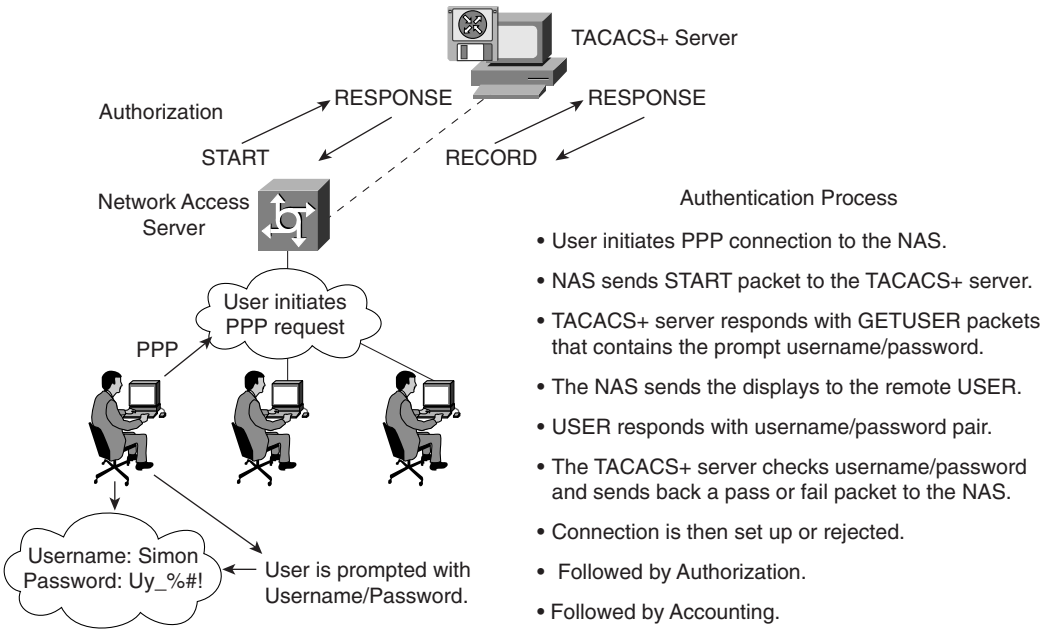
Cisco has also developed Cisco Secure Access Control Server (ACS), a flexible family of security servers that supports both RADIUS and TACACS+. You can even run debugging commands on the Cisco Secure ACS software. In UNIX, you can modify files, such as syslog.conf and csu.cfg, to change the output to your screen. For more details on how to debug on a UNIX server, see http://www.cisco.com/warp/public/480/cssample2x.html#debug.

TACACS+ has the following features:

- TCP packets (port 49) ensure that data is sent reliably across the IP network.
- Supports AAA architectures and, in fact, separates each of the three AAA mechanisms.
- The data between the NAS and server is encrypted.
- Supports both PAP/CHAP and multiprotocols such as IPX and X.25.
- Access control lists (ACL) can be defined on a per-user basis. (RADIUS can also define ACLs on a per-user basis.)

Figure 4-3 displays a typical TACACS+ connection request (authentication).

Figure 4-3 *TACACS+ Authentication Example Sequence*



When a TACACS+ server authenticates a remote user, the following events occur:

1. When the connection is established, the NAS contacts the TACACS+ daemon to obtain a username prompt, which is then displayed to the user. The user enters a username and the NAS and communicates to the TACACS+ server to obtain a password prompt. The NAS displays the password prompt to the user, the user enters a password, and the password is sent to the TACACS+ daemon.
2. The NAS eventually receives one of the following responses from the TACACS+ daemon:
   - **ACCEPT**—The user is authenticated and service can begin. If the NAS is configured to require authorization, authorization begins at this time.
   - **REJECT**—The user has failed to authenticate. The user may be denied further access or may be prompted to retry the login sequence, depending on the TACACS+ daemon.
   - **ERROR**—An error occurred at some time during authentication. This can be either at the daemon or in the network connection between the daemon and the NAS. If an ERROR response is received, the NAS typically tries to use an alternative method for authenticating the user.
   - **CONTINUE**—The user is prompted for additional authentication information.
3. A PAP login is similar to an ASCII login, except that the username and password arrive at the NAS in a PAP protocol packet instead of being typed in by the user, so the user is not prompted. PPP CHAP logins are also similar, in principle.
4. Following authentication, the user is required to undergo an additional authorization phase, if authorization has been enabled on the NAS. Users must first successfully complete TACACS+ authentication before proceeding to TACACS+ authorization.
5. If TACACS+ authorization is required, the TACACS+ daemon is again contacted and it returns an ACCEPT or REJECT authorization response. If an ACCEPT response is returned, the response contains data in the form of attributes used to direct the EXEC or NETWORK session for that user, determining services that the user can access.

   Services include the following:

   - Telnet, rlogin, PPP, SLIP, or EXEC services
   - Connection parameters, including the host or client IP address, ACL, and user timeouts

The TACACS+ authorization process is defined as the packet flow between the NAS and the TACACS+ server. The packets exchanged between the NAS and server contain AV pairs. The NAS sends Start packets and the TACACS+ server responds with Response packets. The server can permit, deny, or modify commands requested by the end user. The data (that contains the full list of all username/password pairs) is stored on a local file defining what commands are permitted by the end user, for example.

TACACS+ accounting provides an audit record of what commands were completed. The NAS sends a record of any commands, and the TACACS+ server sends a response acknowledging the accounting record.

Table 4-3 summarizes the main features of TACACS+.

Table 4-3 *Summary of TACACS+ Protocol*

	Feature
TCP	Packets sent between client and server are TCP.
TCP destination port	Port 49.
Attributes	Packet types are defined in TACACS+ frame format as follows: Authentication 0x01 Authorization 0x02 Accounting 0x03
Seq_no	The sequence number of the current packet flow for the current session. The Seq_no starts with 1, and each subsequent packet increments by one. The client sends only odd numbers. The TACACS+ server sends only even numbers.
Encryption method	The entire packet is encrypted. Data is encrypted using MD5 and a secret key that matches both on the NAS (for example, a Cisco IOS router) and the TACACS+ server.
Multiprotocol support	Multiprotocol Support indicates the following are fully supported in non IP networks, multiprotocols such as AppleTalk, NetBIOS, or IPX, along with IP.

Now, examine the TACACS+ configuration tasks required when enabling TACACS+ on a Cisco IOS router.

TACACS+ Configuration Task List

To configure your router to support TACACS+, you must perform the following tasks:

Step 1 Use the **aaa new-model** global configuration command to enable AAA, which must be configured if you plan to use TACACS+. For more information about using the **aaa new-model** command, refer to http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/secur_c/scprt1/scdaaa.htm.

Step 2 Use the **tacacs-server host** command to specify the IP address of one or more TACACS+ daemons:

```
tacacs-server host hostname [single-connection] [port integer] [timeout
integer] [key string]
```

Step 3 Use the **tacacs-server key** command to specify an encryption key to encrypt all exchanges between the NAS and the TACACS+ daemon. This same key must also be configured on the TACACS+ daemon. The actual command is as follows:

```
tacacs-server key key
```

The key should match the one used on the TACACS+ daemon.

Step 4 Use the **aaa authentication** global configuration command to define method lists that use TACACS+ for authentication.

Step 5 Use **line** and **interface** commands to apply the defined method lists to various interfaces.

Step 6 To enable authorization, use the **aaa authorization** global command to configure authorization for the NAS. Unlike authentication, which can be configured per line or per interface, authorization is configured globally for the entire NAS.

Step 7 To enable accounting for TACACS+ connections, use the **aaa accounting** command. Optional commands include the following:

- Configuring AAA server groups (Optional)
- Configuring AAA server group selection based on Dialed Number Identification Service (DNIS) (Optional)
- Specifying TACACS+ authentication (Required)
- Specifying TACACS+ authorization (Optional)
- Specifying TACACS+ accounting (Optional)

Example 4-5 displays a sample configuration of a Cisco router with TACACS+ authentication for PPP.

Example 4-5 *TACACS+ Authentication for PPP Example*

```
aaa new-model
aaa authentication ppp CCIE group tacacs+ local
tacacs-server host 10.1.2.3
tacacs-server key cciesarecool
interface serial 0
 ppp authentication chap pap CCIE
```

The configuration lines in Example 4-5 are defined as follows:

- The **aaa new-model** command enables the AAA security services.
- The **aaa authentication** command defines a method list, CCIE, to be used on serial interfaces running PPP. The keyword **group tacacs+** means that authentication is done through TACACS+. If TACACS+ returns an ERROR during authentication, the keyword **local** indicates that authentication will be attempted using the local database on the NAS. Note that the local database is not used if a REJECT response is received from the security server.

- The **tacacs-server host** command identifies the TACACS+ daemon as having an IP address of 10.1.2.3. The **tacacs-server key** command defines the shared encryption key as cciesarecool.
- The **interface** command selects the line, and the **ppp authentication** command applies the CCIE method list to this line.

Example 4-6 shows how to configure TACACS+ as the security protocol for PPP authentication using the default method list; it also shows how to configure network authorization through TACACS+.

Example 4-6 *Authorization and TACACS+ Example*

```
aaa new-model
aaa authentication ppp default if-needed group tacacs+ local
aaa authorization network default group tacacs+
tacacs-server host 3.3.3.3
tacacs-server key simoniscool
interface serial 0
ppp authentication default
```

The lines in the preceding sample configuration are defined as follows:

- The **aaa new-model** command enables the AAA security services.
- The **aaa authentication** command defines a method list, default, to be used on serial interfaces running PPP. The keyword **default** means that PPP authentication is applied by default to all interfaces. The **if-needed** keyword means that if the user has already authenticated by going through the ASCII login procedure, PPP authentication is not necessary and can be skipped. If authentication is needed, the keyword **group tacacs+** means that authentication is done through TACACS+. If TACACS+ returns an ERROR during authentication, the keyword **local** indicates that authentication will be attempted using the local database on the NAS.
- The **aaa authorization** command configures network authorization via TACACS+.
- The **tacacs-server host** command identifies the TACACS+ daemon as having an IP address of 3.3.3.3.
- The **tacacs-server key** command defines the shared encryption key as simoniscool.
- The **interface** command selects the line, and the **ppp authentication** command applies the default method list to this line.

The source interface used by TACACS+ or RADIUS can be defined when required as follows:

```
ip tacacs source-interface subinterface-name
ip radius source-interface subinterface-name
```

The **source-interface** commands force the security protocol to use a specific interface as the source IP address. For example, it may be a loopback address (remember, it is always active, unlike a physical interface, which may fail or be down) for redundancy purposes in case of a physical interface failure.

Example 4-7 displays a sample configuration where accounting is also enabled.

Example 4-7 *Accounting Example*

```
aaa new-model
aaa authentication ppp default if-needed group tacacs+ local
aaa accounting network default stop-only group tacacs+
tacacs-server host 3.3.3.3
tacacs-server key andrewiscool
interface serial 0
ppp authentication default
```

The lines in the Example 4-7 configuration are defined as follows:

- The **aaa new-model** command enables the AAA security services.
- The **aaa authentication** command defines a method list, default, to be used on serial interfaces running PPP. The keyword **default** means that PPP authentication is applied by default to all interfaces. The **if-needed** keyword means that if the user has already authenticated through the ASCII login procedure, PPP authentication is not necessary. If authentication is needed, the keyword **group tacacs+** means that authentication is done through TACACS+. If TACACS+ returns an ERROR during authentication, the keyword local indicates that authentication will be attempted using the **local** database on the NAS.
- The **aaa accounting** command configures network accounting through TACACS+. In this example, accounting records stop-only, meaning that the session that just terminated will be sent to the TACACS+ daemon whenever a network connection terminates.
- The **interface** command selects the line, and the **ppp authentication** command applies the default method list to this line.

NOTE You can define a group of TACACS+ servers by defining the servers with the IOS commands **tacacs-server host** *ip-address-of-server* and **tacacs-server key** *secret-key*. For example, to define six servers, you would use the following IOS configuration:

```
tacacs-server host 1.1.1.1
tacacs-server host 2.2.2.2
tacacs-server host 3.3.3.3
tacacs-server host 4.4.4.4
tacacs-server host 5.5.5.5
tacacs-server host 6.6.6.6
tacacs-server key ccie
```

If the first server does not respond within a timeout period (the default is 5 seconds), the next server is queried, and so forth.

Typically, the console port is not configured for authorization.

TACACS+ Versus RADIUS

Table 4-4 compares the main differences between TACACS+ and RADIUS.

Table 4-4 *TACACS+/RADIUS Comparison*

	RADIUS	TACACS+
Packet delivery	UDP.	TCP.
Packet encryption	Encrypts only the password in the access-request packet from the client to the server.	Encrypts the entire body of the packet but leaves a standard TCP header.
AAA support	Combines authentication and authorization.	Uses the AAA architecture, separating authentication, authorization, and accounting.
Multiprotocol support	None.	Supports other protocols, such as AppleTalk, NetBIOS, and IPX.
Router management	Can pass a privilege level down to the router, which can then be used locally for command authorization.	Enables network administrators to control which commands can be executed on a router.
Responses	Uses single-challenge response. Combines authentication and authorization.	Uses multiple-challenge response for each of the AAA processes. Uses the AAA architecture and separates each process.

NOTE You can configure both RADIUS and TACACS+ concurrently on a Cisco router provided that you have defined different list names and applied the list to different interfaces.

NOTE You can download and install a trial copy of Cisco Secure ACS for Windows NT/2000 or UNIX. This comes with a built-in RADIUS and TACACS+ server. You also need a Cisco router with Cisco IOS 12.X with one working Ethernet port. This will reinforce your understanding of the AAA concept. For more information, visit the Cisco Secure Software Center at Cisco.com.

The AAA configuration options are numerous, and those presented in this guide are only a small subset of a larger set that you can view online at Cisco.com. Visit the following URL for more quality examples of how AAA, along with RADIUS or TACACS, can be implemented on Cisco IOS routers:

http://www.cisco.com/pcgi-bin/Support/browse/index.pl?i=Technologies&f=774

The IOS **debug** command set for RADIUS and TACACS is extensive. Presented here are some common RADIUS and TACACS debug outputs found in real networks.

Example 4-8 displays a sample output from the **debug aaa authentication** command for a RADIUS login attempt that failed. The information indicates that TACACS is the authentication method used.

Example 4-8 **debug aaa authentication** *Command*

```
R1# debug aaa authentication
14:02:55: AAA/AUTHEN (164826761): Method=RADIUS
14:02:55: AAA/AUTHEN (164826761): status = GETPASS
14:03:01: AAA/AUTHEN/CONT (164826761): continue_login
14:03:01: AAA/AUTHEN (164826761): status = GETPASS
14:03:04: AAA/AUTHEN (164826761): status = FAIL
```

Example 4-9 displays a sample output from the **debug radius** command that shows a successful login attempt (note that newer versions of IOS code may display some differences), as indicated by an Access-Accept message.

Example 4-9 **debug radius** *Command*

```
R1# debug radius
 13:59:02: Radius: IPC Send 0.0.0.0:1645, Access-Request, id 0xB, len 56
13:59:02:         Attribute 4 6 AC150E5A
13:59:02:         Attribute 5 6 0000000A
13:59:02:         Attribute 1 6 62696C6C
13:59:02:         Attribute 2 18 0531FEA3
13:59:04: Radius: Received from 131.108.1.1:1645, Access-Accept, id 0xB, len 26
13:59:04:         Attribute 6 6 00000001
```

Example 4-10 displays a sample output from the **debug radius** command that shows an unsuccessful login attempt, as indicated by an Access-Reject message.

Example 4-10 **debug radius** *Command*

```
R1# debug radius
13:57:56: Radius: IPC Send 0.0.0.0:1645, Access-Request, id 0xA, len 57
13:57:56:         Attribute 4 6 AC150E5A
13:57:56:         Attribute 5 6 0000000A
13:57:56:         Attribute 1 7 62696C6C
13:57:56:         Attribute 2 18 49C28F6C
13:57:59: Radius: Received from 171.69.1.152:1645, Access-Reject, id 0xA, len 20
```

Encryption Technology Overview

When prominent Internet sites, such as http://www.cnn.com, are exposed to security threats, the news reaches all parts of the globe. Ensuring that data crossing any IP network is secure and not vulnerable to threats is one of today's most challenging tasks in the IP storage arena (so much so that Cisco released an entirely new CCIE for the storage networking certification track).

Major problems for network administrators include the following:

- **Packet snooping (eavesdropping)**—When intruders capture and decode traffic, obtaining usernames, passwords, and sensitive data such as salary increases for the year.
- **Theft of data**—When intruders use sniffers, for example, to capture data over the network and steal that information for later use.
- **Impersonation**—When an intruder assumes the role of a legitimate device but, in fact, is not legitimate. The intruder efficiently assumes the role of an authorized user.

The solution to these and numerous other problems is to provide encryption technology to the IP community and enable network administrators to ensure that data is not vulnerable to any form of attack or intrusion. This ensures that data is confidential, authenticated, and has not lost any integrity during the routing of packets through an IP network.

Encryption (user data that is encrypted will require decryption also) is defined as the process by which plain data is converted into ciphered data (a system in which plain-text data is arbitrarily substituted according to a predefined algorithm known as cipertext) so that only the intended recipient(s) can observe the data. Encryption ensures data privacy, integrity, and authentication.

Figure 4-4 displays the basic methodologies behind data encryption.

Figure 4-4 *Encryption Methodologies*

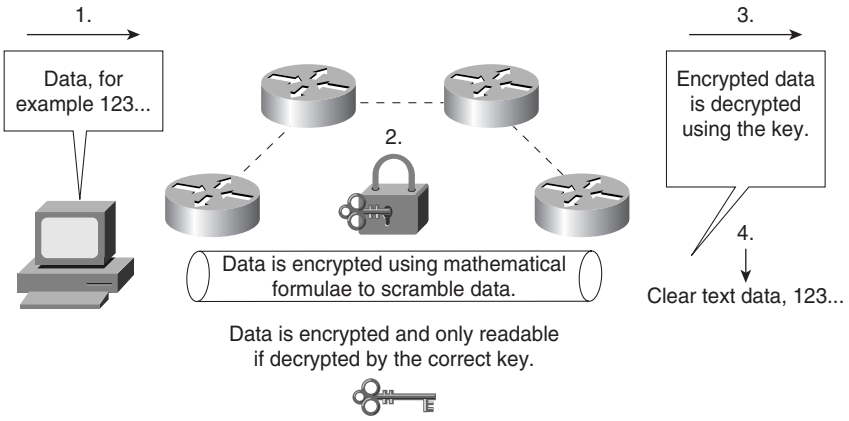


Figure 4-4 demonstrates the basic principles of data encryption, including the following:

1. User data is forwarded over the network.

2. Data (clear text) is modified according to a key. The key is a sequence of digits that decrypts and encrypts messages. Each device has three keys:
   - A private key used to sign messages that is kept secret and never shared.
   - A public key that is shared (used by others to verify a signature).
   - A shared secret key that is used to encrypt data using a symmetric encryption algorithm, such as DES. Typically, however, a device has two keys, a symmetric key and an asymmetric key. The symmetric key is a shared secret that is used to both encrypt and decrypt the data. The asymmetric key is broken into two parts, a private key and a public key.
3. A mathematical formula is applied to scramble the data. In Figure 4-4, the mathematical formula is applied during Step 2.
4. The data flows throughout the network and can be decrypted only if the correct key and algorithm are applied.

Encryption can take place at the application layer, the network layer, or the data link layer. Be aware of the following encryption technologies for the CCIE Security written exam:

- Data Encryption Standard (DES)
- Triple DES (3DES)
- Advanced Encryption Standard (AES)
- IP Security (IPSec)

Cisco IOS routers support the following industry standards to accomplish network layer encryption:

- DES/3DES
- AES
- MD5
- Diffie-Hellman exchange
- IPSec

DES and 3DES

DES is one of the most widely used encryption methods. DES turns clear-text data into cipher text with an encryption algorithm. The receiving station will decrypt the data from cipher text into clear text. The shared secret key is used to derive the session key, which is then used to encrypt and decrypt the traffic.

Figure 4-5 demonstrates DES encryption.

Figure 4-5 *DES Encryption Methodologies*

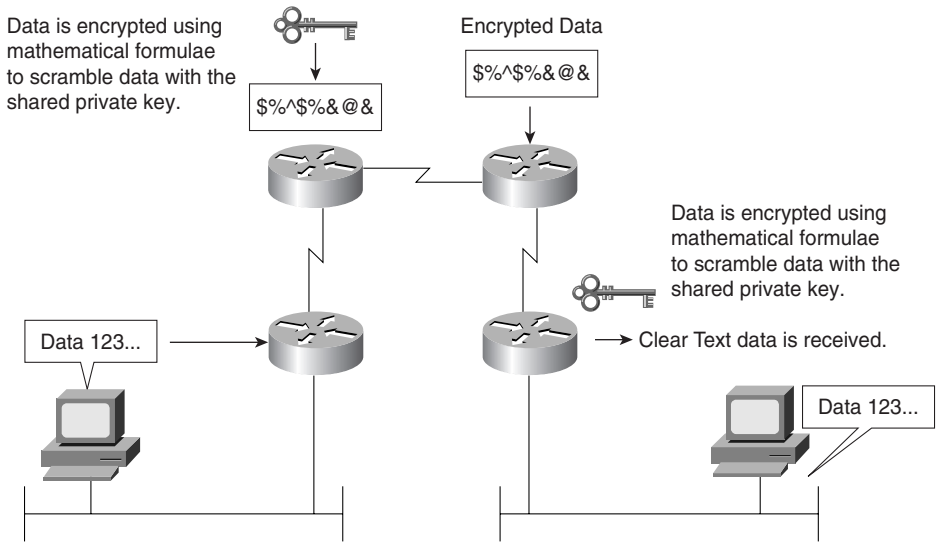


Figure 4-5 demonstrates the PC's clear-text generation. The data is sent to the Cisco IOS router, where it is encrypted with a shared key (remember, the shared secret key is used to derive the session key, which is then used to encrypt and decrypt the traffic) and sent over the IP network in unreadable format until the receiving router decrypts the message and forwards it in clear-text form.

DES is a block cipher algorithm, which means that DES performs operations on fixed-length data streams. DES uses a 56-bit key to encrypt 64-bit datagrams.

DES is a published, U.S. government–standardized encryption method; however, it is no longer a U.S. government–approved encryption algorithm.

3DES is the DES algorithm that performs three times (3 x 3 x encryption and 3 x decryption) sequentially (although there are some variations as well). Three keys are used to encrypt data, resulting in a 168-bit encryption key.

3DES is an improved encryption algorithm standard and is summarized as follows:

1. The sending device encrypts the data with the first 56-bit key.
2. The sending device decrypts the data with the second key, also 56 bits in length.
3. The sending device encrypts for a final time with another 56-bit key.

4. The receiving device decrypts the data with the first key.
5. The receiving device then encrypts the data with the second key.
6. Finally, the receiving device decrypts the data with the third key.

A typical hacker uses a Pentium III computer workstation and takes approximately 22 hours to break a DES key. In the case of 3DES, the documented key-breaking times are approximately 10 billion years when 1 million PC III computers are used. Encryption ensures that information theft is difficult.

TIP It is possible to increase the number of bits in the key, but brute-force cracking of a 1024-bit key is not feasible using current or reasonably foreseeable technology. Even if, based on future innovations, this becomes a weak key length, the value of the data it protects will have very likely diminished to zero. In the event that you have need for more protection, you can increase the key size. However, you should be aware that this will take a processing toll on every secure transaction.

NOTE Unbeknownst to the author of the previous tip, a mathematician named D. J. Bernstein delivered a paper entitled "How To Find Small Factors Of Integers" (http://cr.yp.to/papers.html#nfscircuit) earlier in the year. At the Financial Cryptography conference held in late March, 2002, it was discovered that, using his formulas, 512-bit keys can be broken in less than 10 minutes using Pentium IV–based computers and that an array of them (cost estimate, $1 billion) could break a 1024-bit key in the same time. That price tag is well within the reach of the world's major security agencies; an NSA satellite's price tag is double that, and it has several of them.

The lessons here are two-fold. First, if your data is attractive enough to those able to afford those rapidly declining but still very large price tags, go for the biggest key your software supports. Second, authors who write tips like the previous one do so at great risk.

Encryption can be used to enable secure connections over the LAN, WAN, and World Wide Web.

The end goal of DES/3DES is to ensure that data is confidential by keeping data secure and hidden. The data must have integrity to ensure that it has not been modified in any form, and be authenticated by ensuring that the source or destination is indeed the proper host device. Another encryption standard in common use today is widely regarded as the new industry standard, namely AES.

Advanced Encryption Standard

AES, developed by Joan Daemen and Vincent Rijmen, is a new encryption standard and is considered a replacement for DES. The U.S. government made AES a standard in May 2002, and

the National Institute of Standards and Technology (NIST) has adopted AES. AES provides key lengths for 128, 192, and 256 bits.

AES supports Cipher Blocks Chaining (CBC), which circumvents one of the problems with block algorithms in that two equal plain-text blocks will generate the same two equal ciphertext blocks. With CBC, the key is applied to Plain(1) to get Cipher(1). Then, Cipher(1) is used *as the key* against Plain(2) to get Cipher(2), which is used as the key against Plain(3) to get Cipher(3), continuing on until the end.

AES is designed to be more secure than DES through the following enhancements:

- A larger key size.
- Ensures that the only known approach to decrypt a message is for an intruder to try every possible key.
- Has a variable key length; the algorithm can specify a 128-bit key (the default), a 192-bit key, or a 256-bit key.

NOTE AES is supported in Cisco IOS 12.2.13(T) and later. To enable AES, your router must support IPSec. AES cannot encrypt IPSec and IKE traffic if an acceleration card is present. This restriction will be lifted in a future release of Cisco IOS.

For more details on Cisco IOS support for AES, visit http://cisco.com/en/US/products/sw/iosswrel/ps1839/products_feature_guide09186a0080110bb6.html.

Message Digest 5 and Secure Hash Algorithm

Several hashing algorithms are available. The two discussed here are MD5 and SHA. There is a slight, unknown difference between SHA and SHA-1. NSA released SHA and then later discovered a flaw (undisclosed). NSA fixed it, and called the new version SHA-1. In this guide, SHA refers to SHA-1 also.

Message hashing is an encryption technique that ensures that a message or data has not been tampered with or modified. MD5 message hashing is supported on Cisco IOS routers. A variable-length message is taken, the MD5 algorithm is performed (for example, the **enable secret** *password* command), and a final fixed-length hashed output message called a message digest is produced. MD5 is defined in RFC 1321.

Figure 4-6 displays the MD5 message operation.

Figure 4-6 *MD5 Operation*

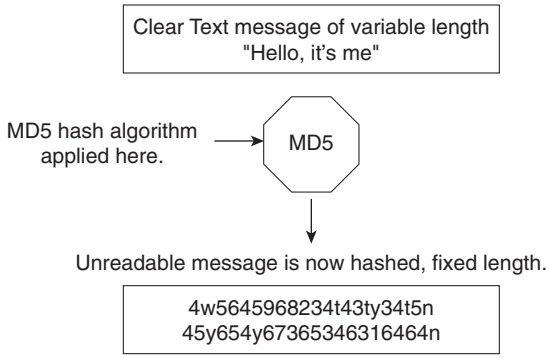


Figure 4-6 displays the simple clear-text message, "Hello, it's me," which can be of any variable length. This message is sent to the MD5 process, where the clear-text message is hashed and a fixed-length, unreadable message is produced. The data can include routing updates or username/password pairings, for example. MD5 produces a 128-bit hash output.

SHA is the newer, more secure version of MD5, and Hash-based Message Authentication (HMAC) provides further security with the inclusion of a key exchange. SHA produces a 160-bit hash output, making it even more difficult to decipher. SHA follows the same principles as MD5 and is considered more CPU-intensive.

For more details on Cisco IOS encryption capabilities, visit the following website:

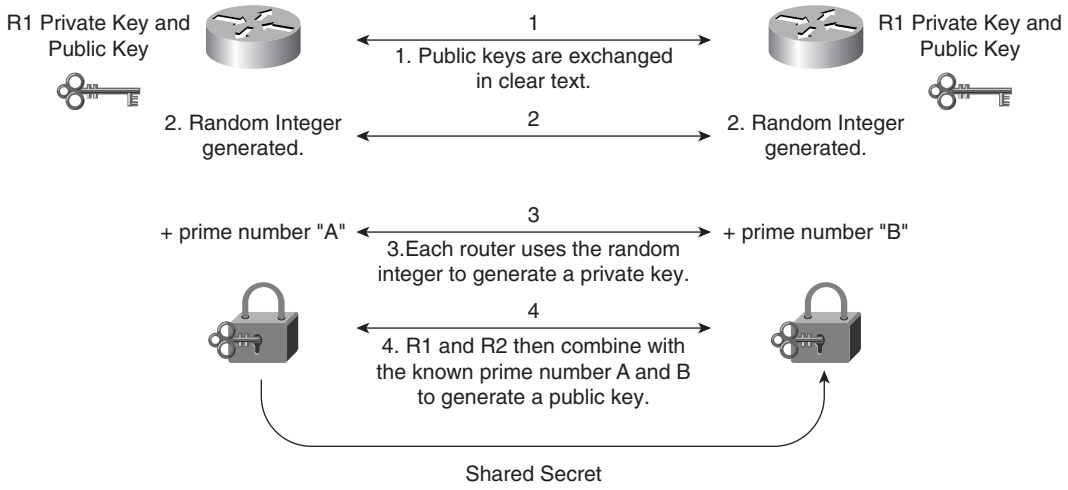
http://www.cisco.com/en/US/products/sw/iosswrel/products_ios_cisco_ios_software_releases.html

Diffie-Hellman

The Diffie-Hellman protocol allows two parties to establish a shared secret over insecure channels, such as the Internet. This protocol allows a secure shared key interchange over the public network, such as the World Wide Web, before any secure session and data transfer is initiated. Diffie-Hellman ensures that, by exchanging just the public portions of the key, both devices can generate a session and ensure that data is encrypted and decrypted by valid sources only. Only public keys (clear text) are exchanged over the public network. Using each device's public key and running the key through the Diffie-Hellmann algorithm generates a common session key. Only public keys will ever be exchanged.

Figure 4-7 displays the Diffie-Hellman exchange between Cisco routers, R1 and R2.

Figure 4-7 *Diffie-Hellman Key Exchange*



The Diffie-Hellman key exchange takes place over a public domain. With the private key kept secret, it is very difficult for an outside intruder to generate the same key, and the private key is never exchanged over the public domain, making the process very secure.

The shared prime numbers (mathematically, a prime number is any positive integer greater than 1 and divisible without a remainder only by 1 and itself) have a special relationship that makes agreeing on a shared secret possible. An analogy would be to have two milkshake blenders making a chocolate milkshake, but with one blender supplied with apples and the other with oranges. The Diffie-Hellman algorithm is the secret ingredient that, when mixed in with both blenders, produces the chocolate milkshake. Remember, it really is a superb algorithm.

NOTE RSA is another public key cryptographic algorithm (named after its inventors, Rivest, Shamir, and Adleman) with a variable key length. RSA's main weakness is that it is significantly slow to compute compared to popular secret-key algorithms, such as DES or 3DES. The Cisco IKE implementation uses a Diffie-Hellman exchange to get the secret keys. This exchange can be authenticated with RSA (or preshared keys). With the Diffie-Hellman exchange, the DES key never crosses the network, which is not the case with the RSA encryption and signing techniques. RSA is public domain like DES/3DES, and to apply RSA, you must be licensed from RSA Data Security. RSA is also approved by the U.S. government. An RSA signature is defined as the host (for example, PC or routers) public and private key, which is bound with a digital certificate. With RSA, only the public key is ever transmitted—the private key is never shared.

IP Security

IPSec provides security services at the IP layer by enabling a system to select required security protocols, determine the algorithm(s) to use for the service(s), and put in place any cryptographic keys required to provide the requested services.

–RFC 2401, "Security Architecture for the Internet Protocol"

IPSec is a defined encryption standard that encrypts the upper layers of the OSI model by adding a new predefined set of headers. IPSec is not just an encryption standard; IPSec provides a variety of other services, as discussed in this section. A number of RFCs defined IPSec.

IPSec is a mandatory requirement for IP version 6 (IPv6 is not covered in the examination). IPSec ensures that the network layer of the OSI model is secured. In TCP/IP's case, this would be the IP network layer. The two IPSec frame formats available, Authentication Header (AH) and Encapsulating Security Payload (ESP), both have protocol numbers assigned to them. They are shimmed in between IP and transport. (The protocol number says to give the datagram to AH or ESP, each of which has a next protocol number that eventually delivers the datagram to TCP or UDP or whatever else might be at the higher layer, such as OSPF.) Therefore, IPSec ensures that the data and headers above the network layer are secured.

IPSec can be configured in two protection modes, which are commonly referred to as security associations (SA). These modes provide security to a given IP connection. The modes are as follows (you have to use IPSec in tunnel mode if you want to obscure the network layer):

- **Transport mode**—Protects payload of the original IP datagram; typically used for end-to-end sessions
- **Tunnel mode**—Protects the entire IP datagram by encapsulating the entire IP datagram in a new IP datagram

An SA is required for inbound and outbound connections. In other words, IPSec is unidirectional. IKE, discussed in this chapter, allows for bidirectional SAs.

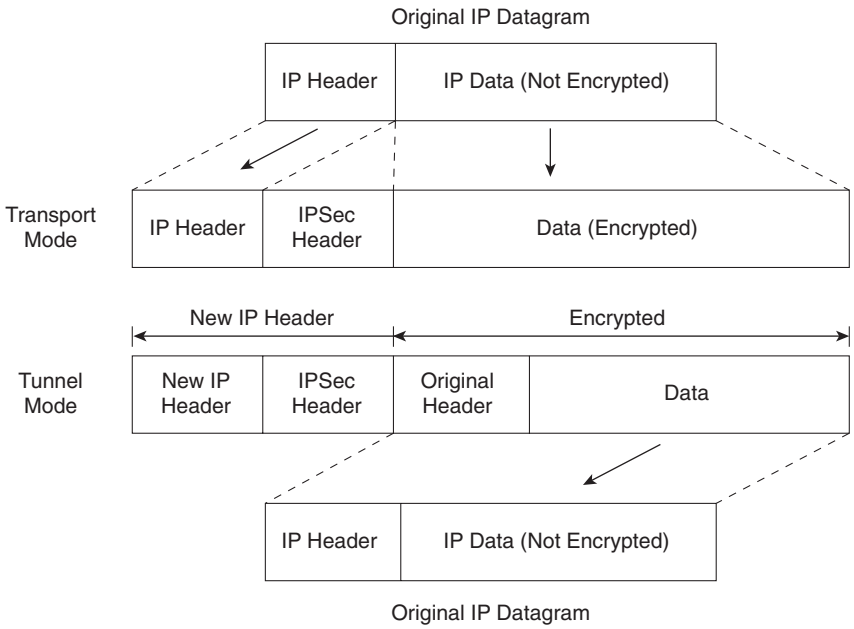
Figure 4-8 displays the extension to the current IP packet frame format for both transport and tunnel modes.

The Encapsulating Security Payload (labeled IPSec header in Figure 4-8) can be of [the] form:

- ESP
- AH

Each of these is discussed in the following sections.

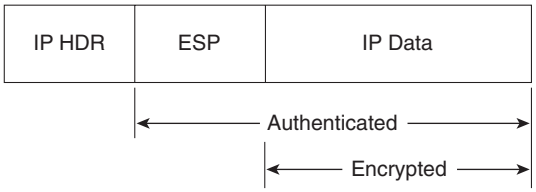
Figure 4-8 *IPSec Protection Modes*



Encapsulating Security Payload

The ESP security service is defined in RFC 2406. ESP provides a service to the IP data (payload), including upper-layer protocols such as TCP. The destination IP number is 50. The ESP header is located between the user data and original IP header, as displayed in Figure 4-9.

Figure 4-9 *ESP Header*



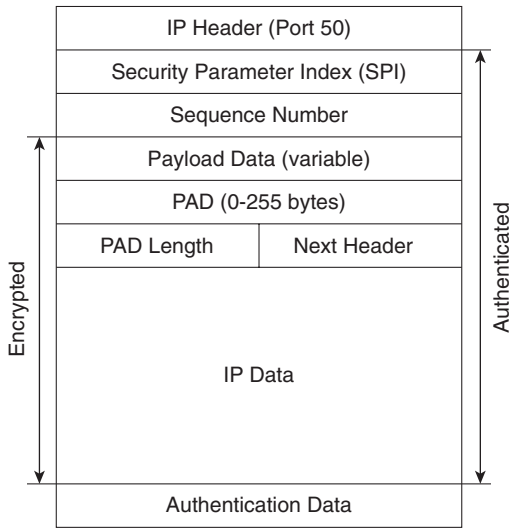
ESP does not encrypt the original IP header (when in transport mode), and encrypts only the IP data by placing a header in between the original IP header and data. ESP provides data confidentiality, data integrity, and data origin authentication. ESP also prevents replay attacks. Replay attacks can include intruders capturing a valid packet and replaying it over the network in an attempt to get a packet conversation between an illegal and legal host.

In tunnel mode ESP, the original IP datagram is placed in the encrypted portion of the Encapsulating Security Payload and that entire ESP frame is placed within a datagram that has unencrypted IP headers. The information in the unencrypted IP headers is used to route the secure datagram from origin to destination. An unencrypted IP routing header might be included between the IP header and the Encapsulating Security Payload.

ESP does not protect the IP header and cannot detect any alternations during packet delivery.

Figure 4-10 displays the frame formats when ESP is applied.

Figure 4-10 *ESP Frame Format*



The Security Parameters Index (SPI) is an arbitrary 32-bit value that, in combination with the destination IP address and security protocol (ESP), uniquely identifies the SA for this datagram.

The Sequence Number, an unsigned 32-bit field, contains a monotonically increasing counter value. It is mandatory and is always present, even if the receiver does not elect to enable the antireplay service for a specific SA. PAD or padding is used when the frame needs to meet the minimum frame size formats. The PAD Length defines the length of padding used. Padding is used for a number of reasons. For example, padding can ensure that the minimum frame size is set so that packets are not discarded because they are too small. Padding is typically all binary ones (1111. . .) or zeros (0000. . .). The sequence number ensures that no intruder or intruders can replay data transactions by using any form of attack mechanisms.

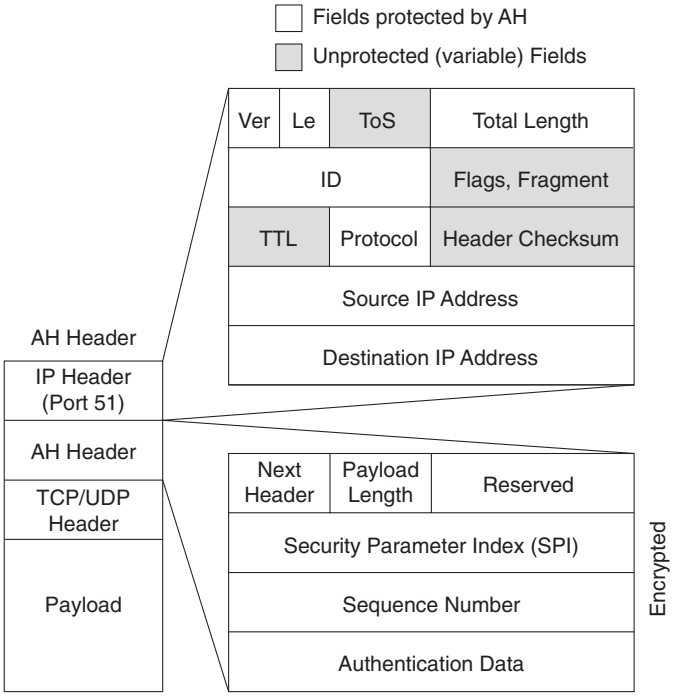
The Next Header is an 8-bit field that identifies the type of data contained in the Payload Data field. The IP Data field contains the data to be sent. The Authentication Data field is a variable-length field containing an Integrity Check Value (ICV) computed over the ESP packet minus the Authentication Data.

Authentication Header

AH is described in RFC 2402. The IP destination protocol is 51. Figure 4-11 highlights the fields in the IP datagram that are encrypted (data is not encrypted) and authenticated. Note that not all fields, such as the Time to Live fields, are encrypted.

> **NOTE** AH provides data origin authentication and optional replay-detection services. AH doesn't provide data confidentiality (or encryption). Authentication is done by applying a one-way hash to create a message digest of the packet. Replay detection can be implemented by using the sequence number in the AH packet header.

Figure 4-11 *AH Header (Tunnel Mode)*



Following is a description of an AH packet:

- Next Header, an 8-bit field, identifies the type of the next payload after the Authentication Header.
- The Payload Length field is an 8-bit field specifying AH's length in 32-bit words (4-byte units), minus 2.
- The Reserved field is a 16-bit field reserved for future use. It *must* be set to 0.

- The SPI is an arbitrary 32-bit value that, in combination with the destination IP address and security protocol (AH), uniquely identifies the SA for this datagram.

AH can operate in transport or tunnel mode; however, unlike ESP, AH also protects fields in the outer IP header (in transport mode, this is the original IP header; in tunnel mode, this is the newly added IP header), which are normally considered nonvariable. AH ensures that if the original IP header has been altered, the packet is rejected. The protection mechanism thereby with AH is authentication only.

Before you take a look at how IPSec is enabled on Cisco routers, you need to understand how keys are exchanged between secure devices to ensure that data is not compromised. IPSec ensures that once an IPSec tunnel is created, the keys are modified so that intruders cannot replicate the keys and create IPSec tunnels to insecure locations. A recent study showed that a network of computer hackers was able to decipher a DES-encrypted message in just a day. (For details on this study please download ants.dif.um.es/~humberto/ asignaturas/v30/docs/CryptographyFAQ.pdf.)

In IPSec, key exchange is provided by Internet Key Exchange (IKE).

Internet Key Exchange

In IPSec, an SA between any two devices will contain all relevant information, such as the cryptographic algorithm in use. A cryptographic algorithm is the product of the science of cryptography. This field of science includes the exact details of encryption algorithms, digital signatures, and key agreement algorithms.

A simple two-router network requires two SAs, one for each router. (IPSec requires one SA on each router for two-way communication.)

Clearly, for a large network, this would not scale. IKE offers a scalable solution to configuration, and key exchange management.

IKE was designed to negotiate and provide authenticated keys in a secure manner. IKE has two phases. In phase I, the cryptographic operation involves the exchange of a master secret where no security is currently in place. IKE phase I is primarily concerned with establishing the protection suite for IKE messages. Phase I operations are required infrequently and can be configured in two modes of operation—aggressive mode and main mode.

Aggressive mode eliminates several steps during IKE authentication negotiation phase I between two IPSec peers. Aggressive mode is faster than main mode but not as secure. Aggressive mode is a three-way packet exchange, while main mode is a six-way packet exchange.

IKE can be configured in aggressive mode or main mode (not both). Aggressive mode is a less-intensive process that requires only three messages to establish a tunnel, versus the six messages required in main mode. Aggressive mode is typically used in remote-access VPN environments.

NOTE Cisco devices use main mode but can respond to peers using aggressive mode. Cisco IOS 12.2T and 12.3 now support configurable options as well.

IKE Phase I Message Types 1–6

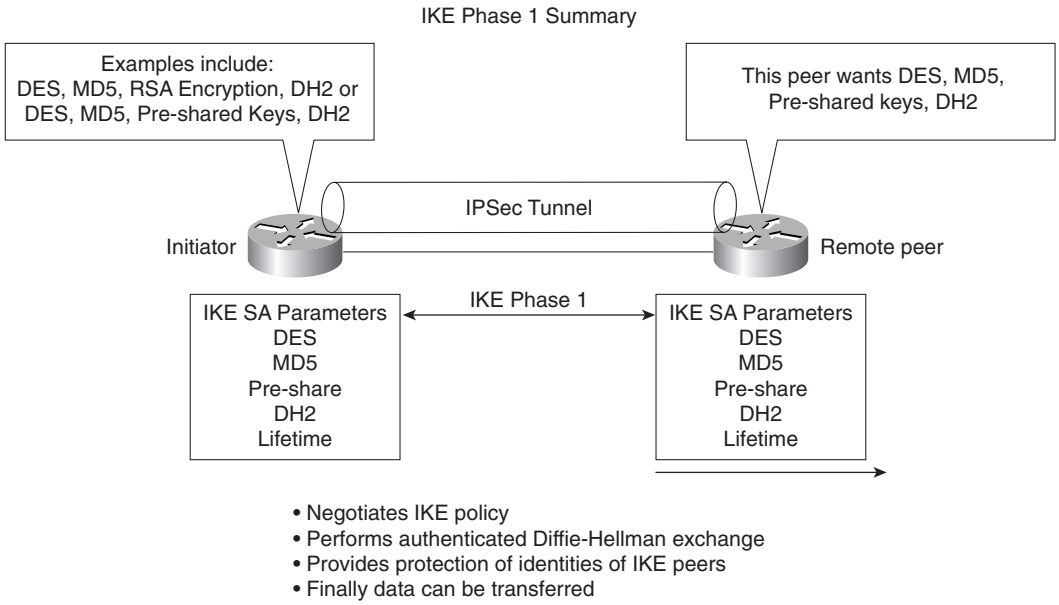
IKE phase I completes the following tasks:

- Main mode negotiates IKE policy (message types 1 and 2). Information exchanges in these message types include IP addresses. Proposals, such as Diffie-Hellman group number and encryption algorithm, are also exchanged here. All messages are carried in UDP packets with a destination UDP port number of 500. The UDP payload comprises a header, an SA payload, and one or more proposals. Message type 1 offers many proposals, and message type 2 contains a single proposal. For message type 2, it is the single proposal and transform that the responder wishes to accept.
- Performs authenticated Diffie-Hellman (DH) exchange. Message types 3 and 4 carry out the DH exchange. Message types 3 and 4 contain the key exchange payload, which is the DH public value and a random number (called a *nonce*). Message types 3 and 4 also contain the remote peer's public key hash and the hashing algorithm. A common session key created on both ends, and the remaining IKE messages exchanged from here are encrypted. If perfect forward secrecy (PFS) is enabled, another DH exchange will be completed. The public key hash and hashing algorithm are sent only if the authentication mechanism is public key encryption.
- Protects IKE peers' identities—identities are encrypted. Message types 5 and 6 are the last stage before traffic is sent over the IPSec tunnel. Message type 5 allows the responder to authenticate the initiating device. Message type 6 allows the initiator to authenticate the responder. These message types are not sent as clear text. Message types 5 and 6 will now be encrypted using the agreed-upon encryption methods established in message types 1 and 2.

After IKE phase I is completed, each peer or router has authenticated itself to the remote peer, and both have agreed on the characteristics of all the SA parameters (IKE parameters).

Figure 4-12 summarizes the key components of IKE phase I and some of the possible permutations available on Cisco IOS routers.

Figure 4-12 *IKE Phase I Summary*



The first message exchanged offers the remote router a choice of IPSec parameters, such as encryption algorithm, 3DES, MD5, and DH group number, for example. The first message's aim is to negotiate all SA policies.

In the second message (type 2), the responding device indicates which of the IPSec parameters it wants to use in the tunnel between the two devices, including the information required to generate the shared secret and provide authentication details. The final message (type 3; until now no encryption is enabled) authenticates the initiator.

After IKE phase I is complete, IKE phase II is initiated. As discussed in the following section, IKE phase II negotiation has three message types.

IKE Phase II Message Types 1–3

IKE phase II negotiates the SA and the keys that will be used to protect the user data. IKE phase II messages occur more frequently, typically every few minutes, whereas IKE phase I messages might occur once a day. On most Cisco IOS devices, the timeout is 1 hour.

IP datagrams that exchange IKE messages use UDP (connectionless) destination port 500.

Phase II negotiations occur in a mode called Oakley quick mode and have three different message exchanges. Quick mode can be the following:

- **Without key exchange**—No PFS is enabled.
- **With key exchange**—When PFS is enabled, the DH algorithm is run once more to generate the shared secret.

Message type 1 allows the initiator to authenticate itself, and selects a random (nonce) number and proposes an SA to the remote peer. Additionally, a public key is provided (can be different than a key exchanged in IKE phase I). IKE phase II message type 2 allows the responding peer to generate the hash. Message type 2 allows the responder to authenticate itself, and selects a random number and accepts the SA offered by the initiating IPSec peer. A hash is intended as a collision-resistant function, as required for the hashing of information prior to application of a signature function.

IKE message type 3 acknowledges information sent from quick mode message type 2 so that the phase II tunnel can be established.

NOTE Perfect forward secrecy can be requested as part of the IKE SA. PFS ensures that a given IPSec SA key was not derived from any other secret. In other words, if someone were to break a key or get the key used between two peers, PFS ensures that the attacker would not be able to derive any other key. If PFS was not enabled, someone could hypothetically break the IKE SA secret key, copy all the IPSec-protected data, and use knowledge of the IKE SA secret to compromise the IPSec SA's setup by this IKE SA. With PFS, breaking IKE would not give an attacker immediate access to IPSec. The attacker would have to break each IPSec SA individually.

Changing the secret key being used for encryption after some period of time (or after a specified number of bytes have been encrypted) is a good idea. Changing keys makes it more difficult for an attacker to derive the key or the newly created key.

Now that all the required data has been exchanged, the initiating IPSec router, or peer, sends a final phase I message with the hash of the two random numbers generated and the message ID. The responder needs to verify the hash before data can be protected.

Figure 4-13 summarizes the key components of IKE phase II.

Figure 4-13 *IKE Phase II Summary*

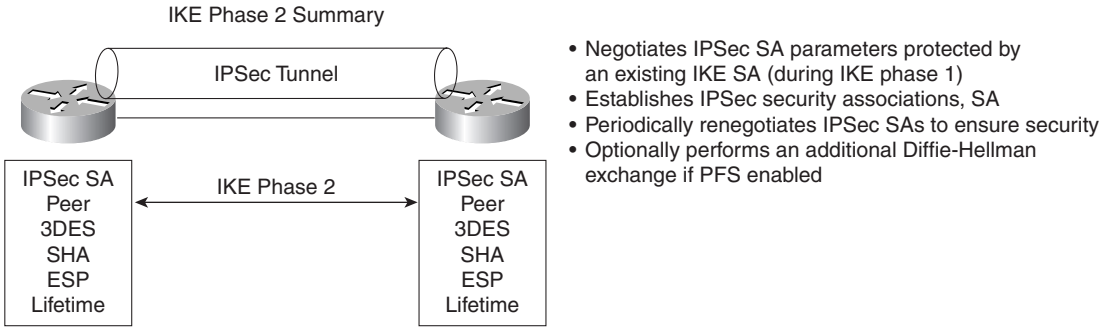


Figure 4-14 displays a typical IKE phase I/II completion.

Figure 4-14 *IKE Phase I/II*

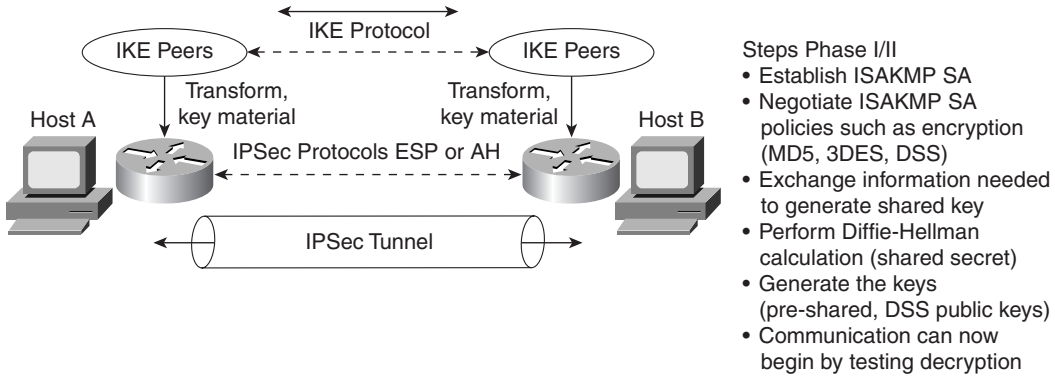


Table 4-5 summarizes the key components of IKE phases I and II.

Table 4-5 *IKE Phases I and II*

Phase	Tasks
IKE phase I	Authenticates IPSec peers Negotiates matching policy to protect IKE exchange Exchanges keys via Diffie-Hellman Establishes the IKE SA
IKE phase II	Negotiates IPSec SA parameters by using an existing IKE SA Establishes IPSec security parameters Periodically renegotiates IPSec SAs to ensure security and that no intruders have discovered sensitive data Can also perform optional additional Diffie-Hellman exchange

IKE requires that all information exchanges be encrypted and authenticated. In addition, IKE is designed to prevent the following attacks:

- **Denial of service**—When messages are constructed with unique cookies that can be used to identify and reject invalid messages.
- **Man in the middle**—Prevents the intruder from modifying messages and reflecting them back to the source or replaying old messages.

NOTE Access control lists determine what traffic to encrypt. For example, you can specify that certain networks are to be encrypted and other networks are not. The **permit** statement encrypts data, and the **deny** statement (implicit) in an ACL does not send traffic encrypted. An ACL applied to IPSec configuration parameters does not stop IP routing on a Cisco IOS router.

Table 4-6 summarizes the key terms and concepts used in IPSec terminology.

Table 4-6 *Summary of IPSec Terms and Concepts*

Term	Meaning
Internet Key Exchange (IKE)	Provides utility services for IPSec, such as authentication of peers, negotiation of IPSec SAs, and encryption algorithms. IKE operates over the assigned UDP port 500.
Security associations (SAs)	Connections between IPSec peers. Each IPSec peer maintains an SA database containing parameters, such as peer addresses, security protocols, and a Security Parameter Index (SPI). An SA is unidirectional, and two SAs are required to form a complete tunnel.
Data Encryption Standard (DES)	Encrypts and decrypts data. It is not considered a strong algorithm and was replaced by 3DES. DES supports only a 56-bit key. 3DES supports three 56-bit keys, or a 168-bit key.
Triple DES (3DES)	A variant of DES that is a much stronger encryption method and uses a 168-bit key.
Advanced Encryption Standard (AES)	A new standard that supports 128-, 192-, and 256-bit key lengths; considered a replacement for DES.
Message Digest version 5 (MD5)	A hash algorithm (128 bit) that takes an input message (of variable length) and produces a fixed-length output message. IKE uses MD5 for authentication purposes.
Secure Hash Algorithm (SHA-1)	A hash algorithm (160 bit) that signs and authenticates data. It is stronger than MD5 but more CPU-intensive and, therefore, slower.
RSA signatures	RSA is a public-key encryption system used for authentication. Users are assigned both private and public keys. The private key is not available to the public and decrypts messages created with the public key. To obtain a legitimate signature, you need to have a Certificate Authority sign your public key, making it a certificate.

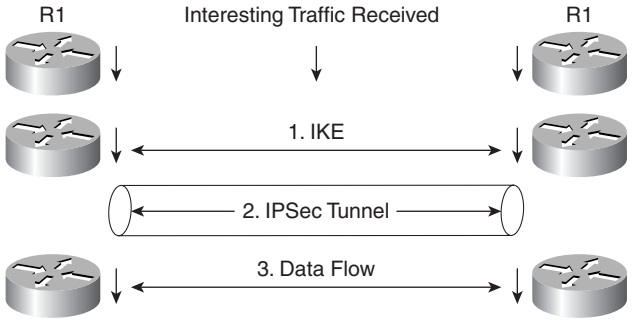
continues

Table 4-6 *Summary of IPSec Terms and Concepts (Continued)*

Term	Meaning
Certificate Authority (CA)	A trusted third party whose purpose is to sign certificates for network entities that it has authenticated.
Diffie-Hellman (DH)	Algorithm that is used to initiate and secure the session between two hosts, such as routers.
Encapsulating Security Payload (ESP)	ESP (transport mode) does not encrypt the original IP header, and only encrypts the IP data by placing a header in between the original IP header and data. ESP (tunnel and transport modes) provides data confidentiality, data integrity, and data origin authentication.

Figure 4-15 displays the flow chart before any data can be transferred between two IPSec peers.

Figure 4-15 *IPSec Flow*



In Figure 4-15, interesting traffic (or traffic from an end user, for example, defined in the ACLs) triggers IKE phases I and II followed by the establishment of the IPSec tunnel. After the IPSec tunnel is established, the data can be transferred. After the data is transferred, the IPSec tunnel is closed. You can tunnel any form of data across the IPSec tunnel, such as IP, Novel IPX, or AppleTalk.

Cisco IOS IPSec Configuration

To enable IPSec between Cisco IOS routers, the following steps are required:

Step 1 Enable Internet Security Association Key Management Protocol (ISAKMP) with the IOS command **crypto isakmp enable**.

This step globally enables or disables ISAKMP at your peer router.

ISAKMP is enabled by default (ACLs define what interesting traffic will be encrypted using defined ACLs).

Step 2 Define an ISAKMP policy, a set of parameters used during ISAKMP negotiation:

```
crypto isakmp policy priority
```

You will enter **config-isakmp** command mode.

Options available include the following:

```
Router(config-isakmp)#?
authentication {rsa-sig | rsa-encr | pre-share}
  default
  encryption {des} {3des} {aes}
  exit
  group 1 2 5
  hash {md5 | sha}
  lifetime seconds
  no
```

This command invokes the ISAKMP policy configuration (**config-isakmp**) command mode. While in ISAKMP policy configuration command mode, the following commands are available to specify the parameters in the policy:

- **encryption** (IKE policy)—The default is 56-bit DES-CBC. To specify the encryption algorithm within an IKE policy, options are **des, 3des**, or **aes**.
- **hash** (IKE policy)—The default is SHA-1. To specify the hash algorithm within an IKE policy, options are **sha**, which specifies SHA-1 (HMAC variant) as the hash algorithm, or **md5**, which specifies MD5 (HMAC variant) as the hash algorithm. Hashed Message Authentication Code (HMAC) uses keyed message digest functions to authenticate a message. The technique used in IPSec is defined in RFC 2104.
- **authentication** (IKE policy)—The default is RSA signatures. To specify the authentication method within an IKE policy, options are **rsa-sig**, which specifies RSA signatures as the authentication method; **rsa-encr**, which specifies RSA encryption as the authentication method; or **pre-share**, which specifies preshared keys as the authentication method.
- **group** {**1** | **2**}—The default is 768-bit Diffie-Hellman. To specify the DH group identifier within an IKE policy, options are **1**, which specifies the 768-bit DH group, or **2**, which specifies the 1024-bit DH group. DH group 5 is also available (1536-bit).
- **lifetime** (IKE policy)—The default is 86,400 seconds (once a day). To specify the lifetime of an IKE SA, use the ISAKMP lifetime policy configuration command. If two IPSec peers share different lifetime values, the chosen value is the shortest lifetime.

Step 3 Set the ISAKMP identity (can be IP address or host name based):

```
crypto isakmp identity {address | hostname}
```

Step 4 Define transform sets (Phase II).

A transform set represents a combination of security protocols and algorithms. During the IPSec SA negotiation, the peers agree to use a particular transform set for protecting a particular data flow.

To define a transform set, use the following commands, starting in global configuration mode:

```
crypto ipsec transform-set
    transform-set-name transform1 [transform2 [transform3]]
```

This command puts you into the crypto transform configuration mode. Then, define the mode associated with the transform set:

```
Router(cfg-crypto-tran)# mode [tunnel | transport]
```

The default is **tunnel**.

Step 5 Define crypto maps, which tie the IPSec policies and SAs together:

```
crypto map name seq method [dynamic dynamic-map-name]
```

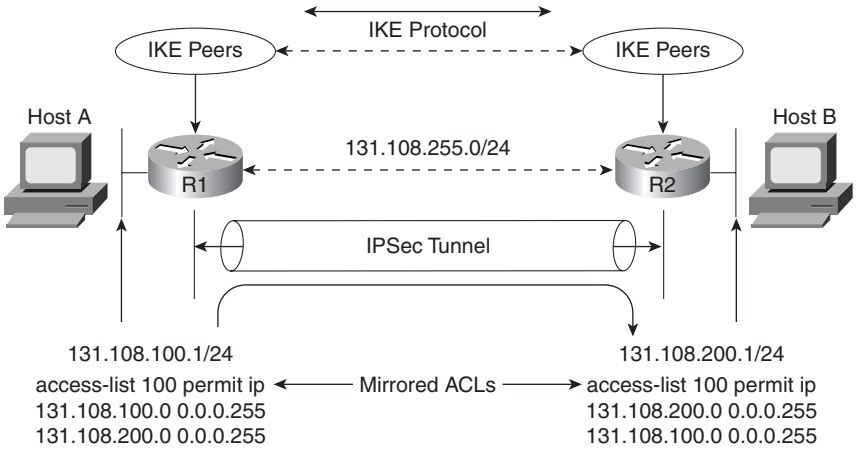
NOTE Crypto map entries created for IPSec pull together the various parts used to set up IPSec SAs, including the following:

- Which traffic should be protected by IPSec (per a crypto ACL).
- The granularity of the flow to be protected by a set of SAs.
- Where IPSec-protected traffic should be sent (who the remote IPSec peer is).
- The local address to be used for the IPSec traffic.
- What IPSec security should be applied to this traffic.
- Whether SAs are manually established or are established through IKE.
- Other parameters that might be necessary to define an IPSec SA.

A dynamic crypto map entry is essentially a crypto map entry without all the parameters configured. It acts as a policy template where the missing parameters are later dynamically configured (as the result of an IPSec negotiation) to match a remote peer's requirements. This allows remote peers to exchange IPSec traffic with the router even if the router does not have a crypto map entry specifically configured to meet all the remote peer's requirements. Dynamic crypto maps are typically used to ensure security between a remote access IPSec client and Cisco IOS router, for example.

The following typical configuration scenario illustrates the IPSec configuration tasks with a two-router network. Figure 4-16 displays two routers configured with the networks 131.108.100.0/24 and 131.108.200.0/24, respectively. Suppose that the Frame Relay cloud is an unsecured network and you want to enable IPSec between the two routers, R1 and R2.

Figure 4-16 *Typical IPSec Topology Between Two Remote Routers*



The network administrator has decided to define the following ISAKMP parameters:

- MD5.
- Authentication will be via preshared keys.
- The shared key phrase is CCIE.
- IPSec mode is transport mode.

To start, configure IKE on Router R1. Example 4-11 displays the IKE configuration on R1. Remember that IKE policies define a set of parameters to be used during IKE negotiation. (Note that in Cisco IOS 12.2T and later, the commands have different options.)

Example 4-11 *R1 IKE Configuration*

```
crypto isakmp policy 1
 hash md5
 authentication pre-share
crypto isakmp key CCIE address 131.108.255.2
```

R1 is configured to use the MD5 algorithm, and the authentication method is defined as preshared. The preshared key value (password) is CCIE, and the remote IPSec peer's address is 131.108.255.2 (R2 serial link to R1 in Figure 4-16).

Preshared Keys Versus Manual Keys

The example shown here is an example of preshared keys whereby IKE is used to negotiate all SA parameters. You can also define IPSec not to use IKE, and this is referred to as *manual IPSec* or *manual keys.* Cisco strongly recommends that you use IKE with preshared keys or RSA signatures, because it is very difficult to ensure that all SA parameters are matching between remote peers. The Diffie-Hellman algorithm is a more secure method when generating secret keys between peers. Manual keys are vulnerable to intruders and unauthorized sources that gain entry to Cisco configuration files. Another major disadvantage of manual keys is that the IOS **crypto map** command used to establish SAs does not expire.

Following the IKE configuration, you can configure IPSec parameters. Example 4-12 enables the IPSec configuration parameters.

Example 4-12 *IPSec Configuration*

```
crypto ipsec transform-set anyname esp-des esp-sha-hmac  mode transport
!
crypto map anyname1 1 ipsec-isakmp
 set peer 131.108.255.2
 set security-association lifetime seconds 900
 set transform-set anyname
 match address 100
!
access-list 100 permit ip 131.108.100.0 0.0.0.255 131.108.200.0 0.0.0.255
```

The transform-set command defines an acceptable combination of security protocols and algorithms. This example applies ESP-DES (ESP with the 56-bit DES encryption algorithm) and ESP with the SHA (HMAC variant) authentication algorithm. (Note that you can also apply 3DES or AES to provide even stronger encryption methods.) The next-hop peer address is defined, and access-list 100 defines what traffic will be encrypted. In Figure 4-16, only IP traffic sourced from 131.108.100.0 destined for 131.108.200.0/24 is sent across the IPSec tunnel.

Example 4-13 displays the configuration on R2.

Example 4-13 *R2 IKE and IPSec Configuration*

```
! IKE configuration
crypto isakmp policy 1
 hash md5
 authentication pre-share
crypto isakmp key CCIE address 131.108.255.1
!
crypto ipsec transform-set anyname esp-des esp-sha-hmac
 mode transport
```

Example 4-13 *R2 IKE and IPSec Configuration (Continued)*

```
!IPSec configuration
crypto map anyname1 1 ipsec-isakmp
 set peer 131.108.255.1
 set security-association lifetime seconds  900
 set transform-set anyname
 match address 100
!Access list defines traffic to be encrypted or interesting traffic
access-list 100 permit ip 131.108.200.0 0.0.0.255 131.108.100.0 0.0.0.255
```

Notice that the routers have mirrored ACLs. This ensures that when encrypted data is received from a source, such as R1, the corresponding IPSec peer router, R2, enables encryption in the reverse direction. For example, when traffic from the network 131.108.100.0/24 residing on Router R1 is sent across, destined for R2's Ethernet network, the IP subnet 131.108.200.0/24, R2 must have a corresponding ACL permitting traffic from the locally connected Ethernet segment, 131.108.200.0/24, to the remote network, the IP subnet on R1, 131.108.100.0/24. This is referred to as mirrored ACLs.

Example 4-13 configures R2 to peer to R1 and only encrypt traffic sourced from 131.108.200.0/24 destined for R1's Ethernet network, 131.108.100.0/24. The crypto predefined map name is anyname1.

Finally, you must apply a previously defined crypto map in Example 4-12. The defined crypto map name is anyname1 in this example, so apply that configuration to the interface. The IOS command that applies the crypto map to an interface is as follows (in config-interface mode):

```
crypto map anyname1
```

Example 4-14 assigns the serial links on R1 and R2 to the crypto map name anyname1 and assigns the crypto map to interface Serial 0/0 on R1/R2.

Example 4-14 *Serial Links and* **crypto map** *on R1/R2*

```
Hostname R1
!
interface Serial0/0
 ip address 131.108.255.1 255.255.255.252
 crypto map anyname1
!
Hostname R2
!
interface Serial0/0
 ip address 131.108.255.2 255.255.255.252
 crypto map anyname1
```

To display the status of all crypto engine active connections, use the IOS command **show crypto engine connections active**.

Example 4-15 displays the current active crypto engines on R1.

Example 4-15 **show crypto engine connections active** *on R1*

```
R1#show crypto engine connections active
 ID Interface       IP-Address      State  Algorithm           Encrypt  Decrypt
  1 Serial0/0       131.108.255.1   set    HMAC_MD5+DES_56_CB        5        5
```

R1 has an IPSec peer connection to R2, through the Serial0/0 interface (131.108.255.1). The algorithm in use is defined and displayed, as well.

To view the crypto map configuration from the PRIV EXEC, use the IOS command **show crypto map**.

Example 4-16 displays the configuration present on R1.

Example 4-16 **show crypto map** *on R1*

```
R1#show crypto map
Crypto Map "anyname1" 1 ipsec-isakmp
 Peer = 131.108.255.2
 Extended IP access list 100
access-list 100 permit ip 131.108.100.0 0.0.0.255 131.108.200.0 0.0.0.255
 Current peer: 131.108.255.2
 Security association lifetime: 4608000 kilobytes/180 seconds
 PFS (Y/N): N
 Transform sets={ anyname, }
 Interfaces using crypto map anyname1:
 Serial0/0
```

Example 4-16 displays the fact that the crypto map named "anyname1" is peered to a remote router, 131.108.255.2, and the access-list 100 defines what traffic will be encrypted across the tunnel.

IPSec is a large field, and to define every possible scenario would require a book in itself. What is presented in this guide is a conceptual overview of IPSec and a common configuration example. For more extensive details, visit:

> http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/fipsenc/index.htm

For the CCIE Security written exam, expect to see scenarios of the variant presented in Figure 4-16 and questions on terminology and the main characteristics of IPSec.

NOTE IPSec can also be supported over the Cisco software tunnel interface. Typically, the tunnel (IP tunnel; GRE, for example) can be configured to carry non-IP traffic by defining a crypto map to the tunnel interface and a crypto control list.

Table 4-7 defines some key IPSec configuration **show** and **debug** commands available on Cisco IOS routers.

Table 4-7 *IOS IPSec Configuration, Show, and Debug Commands*

Command	Description
crypto map *map-name seq-num* **ipsec-isakmp** [**dynamic** *dynamic-map-name*] [**discover**]	Creates a crypto map entry.
crypto ipsec transform-set *transform-set-name transform1* [*transform2* [*transform3*]]	Defines a transform set, an acceptable combination of security protocols and algorithms. This is IKE phase II.
match address [*access-list-id* | *name*]	This command is required for all static crypto map entries. Defines interesting traffic.
crypto dynamic-map *dynamic-map-name dynamic-seq-num*	Use dynamic crypto maps to create policy templates that can be used when processing negotiation requests for new SAs from a remote IPSec peer, even if you do not know all the crypto map parameters.
crypto ca authenticate *name*	This command is required when you initially configure CA support at your router.
crypto ca identity *name*	Use this command to declare a CA.
crypto isakmp enable	Globally enables IKE at your local router.
Show crypto engine connection active	Displays phase I and II SA and traffic sent.
authentication {**rsa-sig** | **rsa-encr** | **pre-share**}	Specifies the authentication method within an IKE policy.
show crypto ipsec sa	Displays the settings used by current SAs to declare a CA.
show crypto map	Displays the crypto map configuration.
show crypto isakmp sa	Displays all current IKE SAs at a peer.
debug crypto engine	Displays debug messages about crypto engines, which perform encryption and decryption.
debug crypto ipsec	Displays IPSec events.
debug crypto pki messages	Displays debug messages for the details of the interaction (message dump) between the CA and the router.
debug crypto isakmp	Enables global IKE debugging.

NOTE A number of PC-based applications are available to the public that allow application layer encryptions.

An excellent e-mail encryption application is a product called Pretty Good Privacy (PGP). Designed and freely available on the Internet (http://www.pgp.com), PGP allows users to authenticate files and e-mail text, allowing only the intended recipient to decrypt the message. Users who send and receive encrypted data exchange keys. With encrypted data, the remote user's key is used to encrypt clear-text data or files. This ensures that the data is authenticated and not forged. Also check out http://www.gnupg.org for a free version of PGP.

Microsoft Outlook 2000 supports PGP and allows the client to encrypt and decrypt data using the preshared public keys.

Certificate Enrollment Protocol

CEP is a protocol jointly developed by Cisco and VeriSign, Inc. CEP is an early implementation of Certificate Request Syntax (CRS), a proposed standard to the IETF. CEP specifies how a device communicates with the CA, how to retrieve the CA's public key, and how to enroll a device with the CA. CEP uses Public Key Cryptography Standards (PKCS).

CEP uses HTTP as a transport mechanism and uses the same TCP port (80) used by HTTP.

NOTE You can find more details on CEP at http://www.cisco.com/warp/public/cc/pd/sqsw/tech/scep_wp.htm. For the CCIE Security lab, the candidate is expected to be able to use common IOS commands such as **crypto ca trustpoint** and know how to enroll certificates**.**

To declare the CA that a Cisco IOS router should use, use the **crypto ca identity** *name* command in global configuration mode. The CA might require a particular name, such as the domain name.

Finally, to cover the exam blueprint, this chapter closes with a short explanation of some of the security protocols used in today's networks to ensure security over wireless connections.

Extensible Authentication Protocol, Protected EAP, and Temporal Key Integrity Protocol

Extensible Authentication Protocol (EAP) enables the dynamic selection of the authentication mechanism at authentication time based on information transmitted in the Access-Request (that is, via RADIUS). PPP also supports EAP during the link establishment phase.

EAP allows the authenticator to request more information before determining the specific authentication mechanism.

A proposal jointly submitted to the IEEE by Cisco Systems, Microsoft, and various other organizations introduced Protected EAP (PEAP), an EAP to provide enhanced functionality and security features to wireless networks. PEAP is today's preferred authentication mechanism in wireless networks.

PEAP provides the following security benefits:

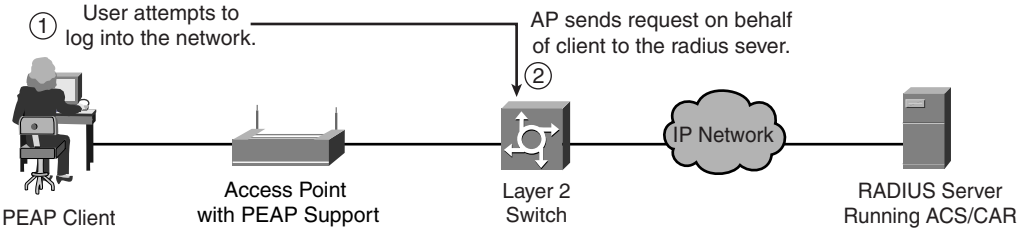
- Relies on Transport Layer Security (TLS) to allow nonencrypted authentication types such as EAP-Generic Token Card (GTC) and One Time Password (OTP) support.
- Uses server-side PKI-based digital certification authentication.
- Allows authentication to an extended suite of directories, including Lightweight Directory Access Protocol (LDAP), Novell NDS, and OTP databases.
- Uses TLS to encrypt all user-sensitive authentication information.
- Supports password change at expiration.
- Does not expose the logon username in the EAP identity response.
- Is not vulnerable to dictionary attacks.

That functionality is provided to wireless client adapters, which may support different authentication types, to communicate with different back-end servers such as RADIUS servers. EAP can be used with wired networks as well.

Microsoft Windows XP supports an extension to EAP, namely Extensible Authentication Protocol Transport Layer Security (EAP-TLS). Hence, a number of options are available to end users so that authentication may be completed securely over a wireless network. Recently Microsoft has added support for EAP-TLS and PEAP to several of its operating systems.

Figure 4-17 displays a typical wireless network in which a user labeled PEAP Client is required to authenticate to either a Cisco Secure ACS or the Cisco Access Registrar. The Cisco Access Registrar is based on a client/server model, which supports AAA. The client passes user information on to the RADIUS server and acts on the response it receives. The server, on the other hand, is responsible for receiving user access requests, authenticating and authorizing users, and returning all of the necessary configuration information the client can then pass on to the user.

Figure 4-17 *PEAP Sample Deployment*



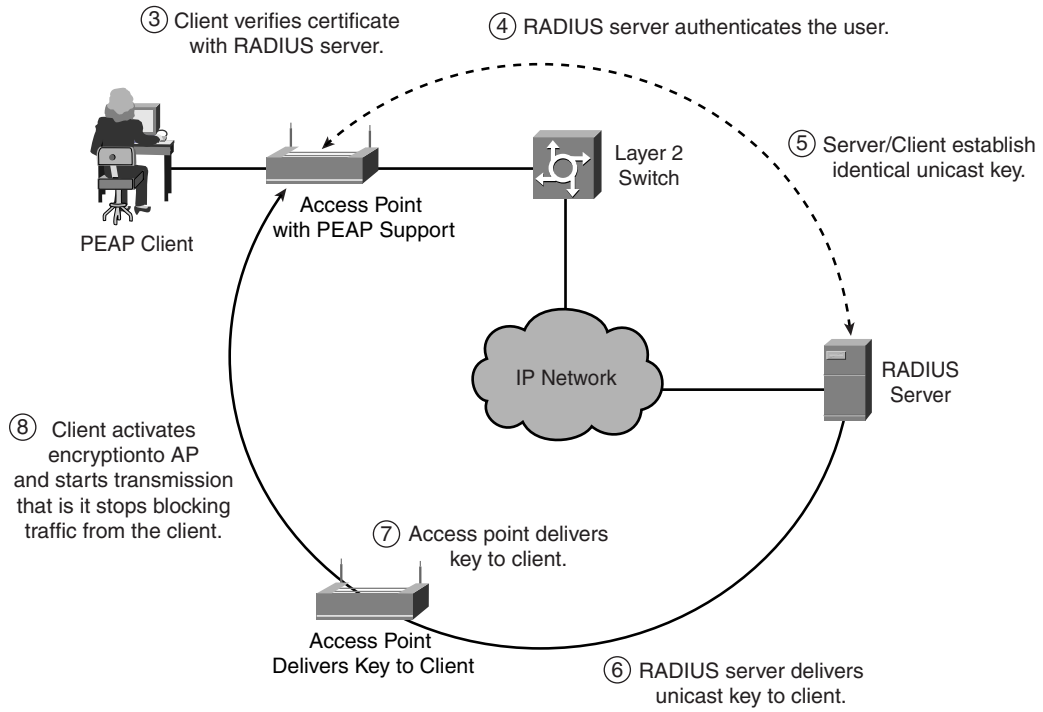
NOTE There have been some additions to EAP to help alleviate some of the weaknesses in other technologies, such as wireless networks.

PEAP is an EAP authentication type that provides mutual authentication of the client and RADIUS server via the access point. PEAP mutual authentication has two parts. In the first part, the server certificate is verified by the client; in the second part, the user is authenticated using the information protected in the TLS tunnel. Additionally, EAP-TLS provides mutual authentication using digital certificates on both the client and the server.

Figure 4-17 displays a Windows XP client trying to associate with a wireless access point—the first step the client performs. The second step is that the access point in Figure 4-17 blocks the request because the client has not been verified by the RADIUS server.

Figure 4-18 displays the next six steps in the PEAP authentication process.

Figure 4-18 *PEAP Authentication Process*



The eight-step process in Figure 4-17 and Figure 4-18 starts with the clients' attempt to authenticate with the RADIUS server. Once a valid username and password are exchanged, the RADIUS server and client establish a common key used to send and receive data over a secured wireless connection.

NOTE Cisco Secure ACS or the Cisco Access Registrar can be used for a combined LEAP and EAP-TLS protocol deployment in an enterprise network. Cisco LEAP is an 802.1X authentication type for wireless LANs that supports mutual authentication between the client and a RADIUS server.

EAP allows the administrator access to a number of password authentication mechanisms, including one-time passwords, public key authentication using smart cards, certificates, and others.

EAP is discussed in RFC 2284, "PPP Extensible Authentication Protocol" (March 1998).

RFC 2284 can be found at http://www.ietf.org/rfc/rfc2284.txt

The Cisco Wireless Security Suite supports IEEE 802.1X authentication and numerous EAP types, including EAP Cisco Wireless (LEAP); EAP-Transport Layer Security (EAP-TLS), and types that operate over EAP-TLS, such as PEAP, EAP-Tunneled TLS (EAP-TTLS), and EAP-Subscriber Identity Module (EAP-SIM). The suite also supports a pre-standard version of Temporal Key Integrity Protocol (TKIP).

TKIP defends against an attack on Wired Equivalent Privacy (WEP) in which the intruder uses an unencrypted segment called the initialization vector (IV) in encrypted packets to calculate the WEP key. TKIP removes the predictability that an intruder relies on to determine the WEP key by exploiting IVs. TKIP protects both unicast and broadcast WEP keys.

TKIP provides enhancements to 128-bit encryption. One such enhancement is *per-packet key hashing*, where the encryption key is changed on each packet. This feature helps combat a common WLAN hacking tool called AirSnort, freely available at http://airsnort.shmoo.com/, which takes advantage of a weakness in WEP encryption when static WEP keys are not changed during a session. It must be pointed out, however, that even with TKIP, the session key needs to be changed before the IV space recycles at 16.7 million packets.

Another important new security advance with TKIP is Message Integrity Check (MIC). With MIC, a digital signature is included with every frame sent, neutralizing the man-in-the-middle attack by hackers who can capture a wireless packet, modify it, and resend it.

TKIP and MIC are easily deployed on an access point. The following list details the simple three-step IOS configuration process:

Step 1 Enter global configuration mode:

```
configuration terminal
```

Step 2 Enter interface configuration mode for the radio interface:

```
interface dot11radio 0
```

Step 3 Enable WEP, MIC, and TKIP:

```
encryption [vlan vlan-id] mode wep {optional [key-hash] ¦ mandatory [mic]
    [key-hash]}
```

Virtual Private Dial-Up Networks (VPDN)

A VPDN is a network that extends remote access dialup clients to a private network. VPDN tunnels use either Layer 2 forwarding (L2F) or Layer 2 Tunnel Protocol (L2TP).

Cisco introduced L2F in RFC 2341. It is also used to forward PPP sessions for Multichassis Multilink PPP.

L2TP, introduced in RFC 2661, combines the best of the Cisco L2F protocol and Microsoft Point-to-Point Tunneling Protocol (PPTP). Moreover, L2F supports only dial-in VPDN, while L2TP supports both dial-in and dial-out VPDN.

Both protocols use UDP port 1701 to build a tunnel through an IP network to forward link-layer frames.

For L2F, the setup for tunneling a PPP session consists of two steps:

Step 1 Establish a tunnel between the NAS and the home gateway (HWY). The HWY is a Cisco router or access server (for example, an AS5300) that terminates VPDN tunnels and PPP sessions. This phase takes place only when no active tunnel exists between both devices.

Step 2 Establish a session between the NAS and the home gateway.

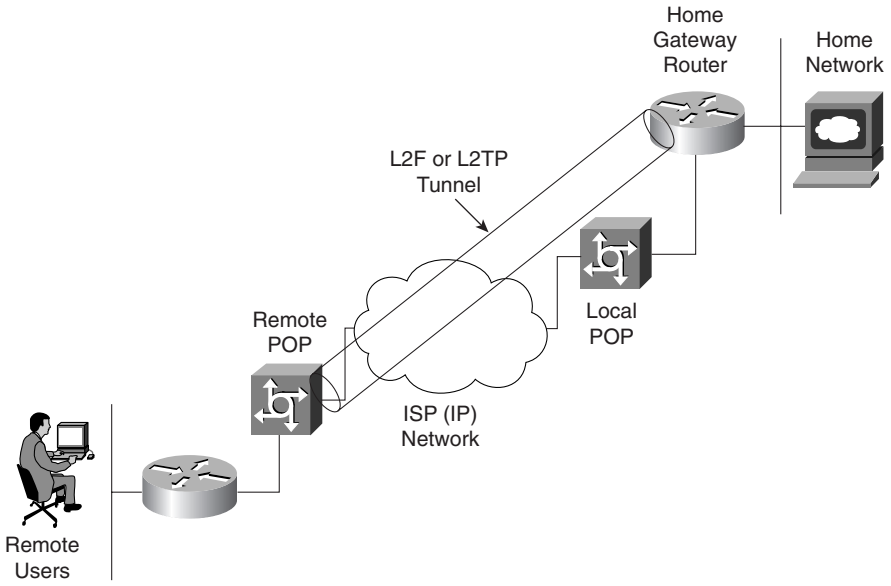
For L2TP, the setup for tunneling a PPP session consists of two steps:

Step 1 Establish a tunnel between the L2TP access concentrator (LAC) and the L2TP network server (LNS). The LAC acts as one side of the L2TP tunnel endpoint and has a peer to the LNS. This phase takes place only when no active tunnel exists between both devices.

Step 2 Establish a session between the LAC and the LNS.

Figure 4-19 displays the tunnel termination points between a remote point of presence (POP) (typically an ISP router) and the home gateway router.

Figure 4-19 *L2F or L2TP Tunnel Termination*



The remote POP accepts frames encapsulated in L2F or L2TP and forwarded over the tunnel.

The LAC and LNS are hardware devices, such as Cisco's AS 5300 series router platform. The LAC's function is to sit between the LNS and the remote system and forward packets to and from each device. The LNS logically terminates the PPP connection.

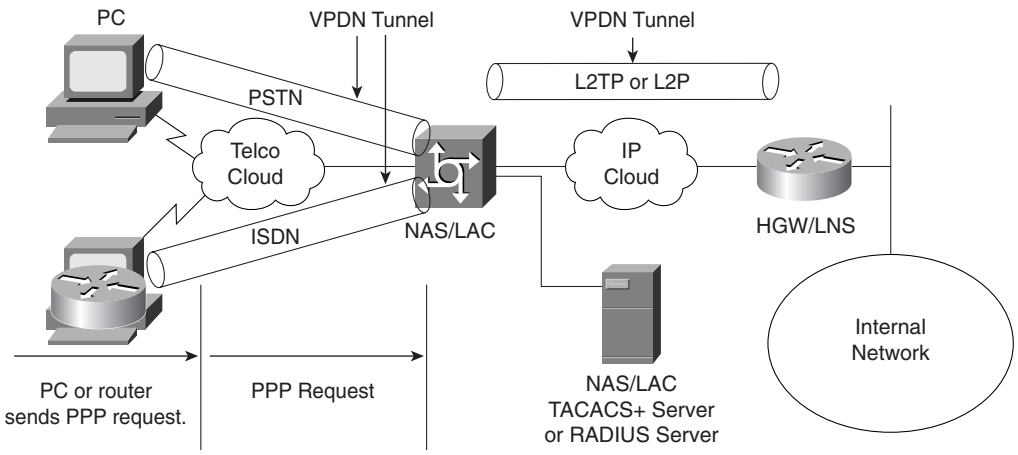
VPDNs are implemented so that users connected through ISPs in any part of the world can take advantage of the connection to the ISP and tunnel the company's remote access traffic through the ISP network.

VPDNs include the following benefits:

- Access to the corporate network from a remote location.
- Offload remote access services to the ISP, which already has the infrastructure place.
- End system transparency because the remote user does not require any hardware or software to use VPDN. Cisco IOS routers performs all the requirements.
- Allows for accounting, which is sent from the home gateway router.

Figure 4-20 displays a typical VPDN scenario where a PC or router dials the NAS/LAC to request a VPDN connection to the private network.

Figure 4-20 *VPDN Network Scenario*



To implement the VPDN configuration, you need the following:

- A Cisco router or access server for client access (NAS/LAC) and a Cisco router for network access (HGW/LNS) with IP connectivity between them.
- Host names of the routers or local names to use on the VPDN groups.
- A tunneling protocol, either the L2TP or L2F Protocol. L2TP is an industry standard, and L2F is a Cisco-proprietary protocol.
- A password for the routers to authenticate the tunnel.
- A tunneling criteria, either domain name or Dialed Number Identification Service (DNIS).
- Username and password for the user (client dialing in).
- IP addresses and keys for your TACACS+ servers.

A VPDN connection between a remote user (router or through PSTN) and the corporate LAN is accomplished in the following steps:

Step 1 The remote user initiates a PPP connection to the ISP using the analog telephone system or ISDN.

Step 2 The ISP's NAS accepts the connection.

Step 3 The ISP NAS authenticates the end user with CHAP or PAP. The username determines whether the user is a VPDN client. If the user is not a VPDN client, the client accesses the Internet or other contacted service.

Step 4 The tunnel endpoints—the NAS and the home gateway—authenticate each other before any sessions are attempted within a tunnel.

Step 5 If no L2F tunnel exists between the NAS and the remote users' home gateway, a tunnel is created. Then, an unused slot within the tunnel is allocated.

Step 6 The home gateway accepts or rejects the connection. Initial setup can include authentication information required to allow the home gateway to authenticate the user.

Step 7 The home gateway sets up a virtual interface. Link-level frames can now pass through this virtual interface through the L2F tunnel.

VPDN Configuration Task List

To configure VPDNs on the home gateway router, complete the following steps:

Step 1 Create a virtual template interface, and enter the interface configuration mode:

```
interface virtual-template number
```

Step 2 Identify the virtual template interface type and number on the LAN:

```
ip unnumbered interface number
```

Step 3 Enable PPP encapsulation on the virtual template interface:

```
encapsulation ppp
```

Step 4 Enable PPP authentication on the virtual template interface:

```
ppp authentication {chap | ppp}
```

Step 5 Enable the global configuration command to allow virtual private networking on the NAS and home gateway routers:

```
vpdn enable
```

Step 6 Specify the remote host (the NAS), the local name (the home gateway) to use for authenticating, and the virtual template to use:

Home gateway router:

```
vpdn incoming nas-name hgw-name virtual-template number
```

NAS configuration:

```
vpdn outgoing domain-name NAS-nameip ip ip-address
```

NOTE You can also enable the NAS to authenticate users via TACACS+ or RADIUS using AAA commands.

A typical configuration file on a UNIX server has a configuration similar to the following configuration:

```
LAC Radius Configuration - Sample
Sanjose.cisco.com   Password = "cisco"
Service-Type = Outbound-User,
cisco-avpair = "vpdn:tunnel-id=DEFGH",
cisco-avpair = "vpdn:tunnel-type=l2tp",
cisco-avpair = "vpdn:ip-addresses=10.31.1.9",
cisco-avpair = "vpdn:l2tp-tunnel-password=ABCDE"
```

The configuration on the LAC defines the specific av-pairs, namely the tunnel-id, tunnel-type, ip-address, and l2tp password.

Example 4-17 displays a typical NAS/LAC configuration using TACACS+.

Example 4-17 *Sample NAS/LAC Configuration*

```
hostname NAS-LAC
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authentication ppp default if-needed group tacacs+
aaa authorization network default group tacacs+
enable password cciesarecool
!
username Melanie password 0 verysecretpassword
!
vpdn enable
!
interface Ethernet0
ip address 131.108.1.1 255.255.255.0
interface Dialer1
Description USER dials in and is assigned this interface
 ip unnumbered Ethernet0
 encapsulation ppp
 dialer-group 1
 peer d\efault ip address pool IPaddressPool
 ppp authentication chap
!
ip local pool IPaddressPool 10.10.10.1 10.10.10.254
!
tacacs-server host 3.3.3.3
tacacs-server key extremelysecrtetpassword
dialer-list 1 protocol ip permit
line con 0
 login authentication CONSOLE
 transport input none
line 1 96
```

Example 4-17 *Sample NAS/LAC Configuration (Continued)*

```
 autoselect during-login
 autoselect ppp
 modem Dialin
line aux 0
line vty 0 4
```

Example 4-17 displays the ISP router that typically supplies the tunnel-id to the HGW and IP address to the dial users.

Example 4-18 displays a typical configuration the home gateway router.

Example 4-18 *Sample HGY/LNS Configuration*

```
hostname HGY-LNS
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authentication ppp default if-needed group tacacs+
aaa authorization network default group tacacs+
enable password cciesarecool
vpdn enable
!
vpdn-group DEFAULTcanbeanyname
! Default L2TP VPDN group
 accept-dialin
  protocol any
  virtual-template 1
 local name LNS
 lcp renegotiation always
 l2tp tunnel password 0 secretpwd
interface Virtual-Template1
 ip unnumbered FastEthernet0/0
 peer default ip address pool IPaddressPool
 ppp authentication chap
ip local pool IPaddressPool 11.11.11.1 11.11.11.254
!
tacacs-server host 3.3.3.3
tacacs-server key easypwd
!
end
```

Foundation Summary

The "Foundation Summary" is a condensed collection of material for a convenient review of this chapter's key concepts. If you are already comfortable with the topics in this chapter and decided to skip most of the "Foundation Topics" material, the "Foundation Summary" will help you recall a few details. If you just read the "Foundation Topics" section, this review should help further solidify some key facts. If you are doing your final preparation before the exam, the "Foundation Summary" offers a convenient and quick final review.

Table 4-8 *AAA Terminology*

Attribute	Meaning
Authentication	Who are you? A remote user must be authenticated before being permitted access to network resources. Authentication allows users to submit their usernames and passwords, and permits challenges and responses. Username/password pairs are a common form of authentication.
Authorization	What resources are you permitted to use? Once the user is authenticated, authorization defines what services in the network the user is permitted access to. The operations permitted here can include IOS privileged EXEC commands.
Accounting	What resources were accessed, at what time, and by whom, and what commands were issued to access them? Accounting allows the network administrator to log and view what was actually performed; for example, if a Cisco router was reloaded or the configuration was changed. Accounting ensures that an audit will enable network administrators to view what was performed and at what time.

Table 4-9 *RADIUS Summary*

Feature	Meaning
UDP	Packets sent between clients and servers are UDP primarily because TCP's overhead does not allow for significant advantages. Typically, the user can wait for a username/password prompt.
UDP destination port	Early deployments of RADIUS used UDP ports 1645 and 1646. The officially assigned port numbers are 1812 and 1813.
Attributes	Attributes are used to exchange information between the NAS and client.
Model	Client/server-based model in which packets are exchanged in a unidirectional manner.
Encryption method	The password is encrypted using MD5; the username is not encrypted. RADIUS encrypts only the password in the access-request packet, sent from the client to the server. The remainder of the packet is in clear text. A third party could capture other information, such as the username, authorized services, and accounting information.
Multiprotocol support	Does not support protocols such as AppleTalk, NetBIOS, or IPX. IP is the only protocol supported.

Table 4-10 *TACACS+ Summary*

Feature	Meaning
TCP	Packets sent between client and server are TCP.
TCP destination port	Port 49.
Attributes	Packet types are defined in TACACS+ frame format as follows: Authentication 0x01 Authorization 0x02 Accounting 0x03
Seq_no	The sequence number of the current packet flow for the current session. The Seq_no starts with 1, and each subsequent packet increments by one. The client sends only odd numbers. TACACS+ servers send only even numbers.
Encryption method	The entire packet is encrypted. Data is encrypted using MD5 and a secret key that matches both on the NAS (for example, a Cisco IOS router) and the TACACS+ server.
Multiprotocol support	Supports protocols such as AppleTalk, NetBIOS, or IPX. IP-supported only.

Table 4-11 *RADIUS Versus TACACS+*

	RADIUS	TACACS+
Packet delivery	UDP	TCP
Packet encryption	Encrypts only the password in the access-request packet from the client to the server.	Encrypts the entire body of the packet, but leaves a standard TCP header.
AAA support	Combines authentication and authorization.	Uses the AAA architecture, separating authentication, authorization, and accounting.
Multiprotocol support	None.	Supports other protocols, such as AppleTalk, NetBIOS, and IPX.
Router management	Can pass a privilege level down to the router, which can then be used locally for command authorization.	Enables network administrators to control which commands can be executed on a router.

Table 4-12 *Encryption Methods*

Encryption Method	Description
Data Encryption Standard (DES)	A block cipher algorithm, which means that it performs operations on fixed-length data streams. Uses a 56-bit key to encrypt 64-bit datagrams. DES is a published, U.S. government–approved encryption algorithm.

continues

Table 4-12 *Encryption Methods (Continued)*

Encryption Method	Description
Triple DES (3DES)	A variant of DES that iterates three times with three separate keys (encrypts with one 56-bit key, decrypts with another 56-bit key, and then encrypts with another 56-bit key). Three keys are used to encrypt data, resulting in a 168-bit encryption key.
Advanced Encryption Standard (AES)	A new standard that replaces DES. Encryption key lengths are 128, 192, and 256 bits.

Table 4-13 *IKE Phase I/II*

Phase	Tasks
IKE phase I	Authenticates IPSec peers Negotiates matching policy to protect IKE exchange Exchanges keys using Diffie-Hellman Establishes the IKE security association
IKE phase II	Negotiates IPSec SA parameters by using an existing IKE SA Establishes IPSec security parameters Periodically renegotiates IPSec SAs to ensure security and that no intruders have discovered sensitive data Can also perform optional additional Diffie-Hellman exchange

Table 4-14 *IPSec Terminology*

Term	Meaning
Internet Key Exchange (IKE)	A protocol that provides utility services for IPSec, such as authentication of peers, negotiation of IPSec SAs, and encryption algorithms.
Security association (SA)	A connection between IPSec peers. An SA is unidirectional, and two SAs are required to form a complete tunnel.
Message Digest 5 (MD5)	A hash algorithm (128 bit) that takes an input message (of variable length) and produces a fixed-length output message. IKE uses MD5 or SHA-1 for authentication purposes.
Secure Hash Algorithm (SHA-1)	A hash algorithm (160 bit) that signs and authenticates data.

Table 4-14 *IPSec Terminology (Continued)*

Term	Meaning
RSA signatures	RSA is a public-key encryption system used for authentication. Users are assigned both private and public keys. The private key is not available to the public and is used to decrypt messages created with the public key. To have a signature validated you need to have a CA sign the public key, making it a certificate.
Certificate Authority (CA)	A trusted third party whose purpose is to sign certificates for network entities it has authenticated.
Authentication Header (AH)	Used to authenticate data. AH provides data origin authentication and optional replay-detection services.
Encapsulating Security Payload (ESP)	ESP (transport mode) does not encrypt the original IP header, and only encrypts the IP data by placing a header in between the original IP header and data. ESP (tunnel and transport modes) provides data confidentiality, data integrity, and data origin authentication.
Diffie-Hellman (DH)	Algorithm that is used to initiate and secure the session between two hosts, such as routers.
Advanced Encryption Standard (AES)	A new encryption standard that is considered a replacement for DES. The U.S. government made AES a standard in May 2002. AES provides key lengths for 128, 192, and 256 bits.

Table 4-15 *Enabling TKIP on an Access Point*

Step 1	Enter global configuration mode: **configuration terminal**
Step 2	Enter interface configuration mode for the radio interface: **interface dot11radio 0**
Step 3	Enable WEP, MIC, and TKIP: **encryption** [**vlan** *vlan-id*] **mode wep** {**optional** [**key-hash**] | **mandatory** [**mic**] [**key-hash**]}

Q & A

The Q & A questions are designed to help you assess your readiness for the topics covered on the CCIE Security written exam and those topics presented in this chapter. This format should help you assess your retention of the material. A strong understanding of the answers to these questions will help you on the CCIE Security written exam. You can also look over the questions at the beginning of the chapter again for further review. As an additional study aid, use the CD-ROM provided with this book to take simulated exams, which draw from a database of over 500 multiple-choice questions.

Answers to these questions can be found in Appendix A, "Answers to Quiz Questions."

1. Define the AAA model and a typical application on a Cisco IOS router.
2. Can you allow a remote user authorization before the user is authenticated with AAA?
3. What IOS command is required when enabling AAA for the first time?
4. What is the privilege level of the following user? Assume AAA is not configured.

   ```
   R2>
   ```

5. Define four possible RADIUS responses when authenticating the user through a RADIUS server.
6. What are RADIUS attributes? Supply five common examples.
7. What protocols does RADIUS use when sending messages between the server and client?
8. What predefined destination UDP port number is RADIUS accounting information sent to?
9. What does the following Cisco IOS software command accomplish on a Cisco IOS router?

   ```
   aaa authentication ppp user-radius if-needed group radius
   ```

10. What is the RADIUS server IP address and key for the following configuration?

    ```
    radius-server host 3.3.3.3
    radius-server key GuitarsrocKthisplaneT
    ```

11. TACACS+ is transported over what TCP server port number?
12. What information is encrypted between a Cisco router and a TACACS+ server?
13. What are the four possible packet types from a TACACS+ server when a user attempts to authenticate a Telnet session to a Cisco router configured for AAA, for example?

14. What is the significance of the sequence number in the TACACS+ frame format?

15. What does the following IOS command accomplish?

```
aaa authentication ppp default if-needed group tacacs+ local
```

16. What IOS command defines the remote TACACS+ server?

17. What are the major difference between TACACS+ and RADIUS?

	RADIUS	TACACS+
Packet delivery	UDP	TCP
Packet encryption	Encrypts only the password in the access-request packet from the client to the server.	Encrypts the entire body of the packet but leaves a standard TCP header.
AAA support	Combines authentication and authorization. Accounting is handled differently.	Uses the AAA architecture, separating authentication, authorization, and accounting.
Multiprotocol support	None.	Supports other protocols, such as AppleTalk, NetBIOS, and IPX.
Router management	Does allow users to control which commands can be executed on a router. Can pass a privilege level down to the router, which can then be used locally for command authorization.	Enables network administrators to control which commands can be executed on a router.

18. What are the three most common threats from intruders that network administrators face?

19. What is a hash in encryption terminology?

20. Name the two modes of operation in IPSec and their characteristics.

21. What does IKE accomplish?

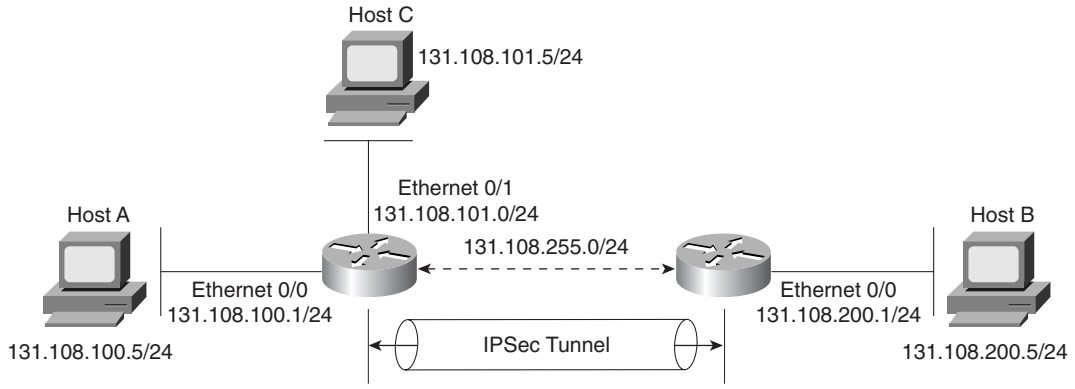
22. Certificate Enrollment Protocol is transported over what TCP port?

Scenario

Scenario: Configuring Cisco Routers for IPSec

Figure 4-21 displays a simple two-router topology where traffic from network 131.108.100.0/24 is encrypted when it is sent to the remote network 131.108.200.0/24.

Figure 4-21 *Scenario Topology*



Example 4-19 displays the working configuration of R1, with lines numbered from 1 to 31.

Example 4-19 *R1's Full Configuration*

```
1.  version 12.2
2.  hostname R1
3.  enable password cisco
4.  crypto isakmp policy 1
5.   hash md5
6.   authentication pre-share
7.  crypto isakmp key CCIE address 131.108.255.2
8.  crypto ipsec transform-set anyname esp-des esp-sha-hmac
9.  mode tunnel
10. crypto map anyname1 1 ipsec-isakmp
11.  set peer 131.108.255.2
12.  set security-association lifetime seconds 180
13.  set transform-set anyname
14.  match address 100
15. interface Ethernet0/0
16.  ip address 131.108.100.1 255.255.255.0
17. interface Serial0/0
18. ip address 131.108.255.1 255.255.255.252
```

Example 4-19 *R1's Full Configuration (Continued)*

```
 encapsulation frame-relay
 ip split-horizon
 ip ospf network point-to-point
 frame-relay map ip 131.108.255.2 102 broadcast
 frame-relay interface-dlci 102
 frame-relay lmi-type ansi
 crypto map anyname1
interface Ethernet0/1
 ip address 131.108.101.1 255.255.255.0
router ospf 1
 network 131.108.0.0 0.0.255.255 area 0
 access-list 100 permit ip 131.108.100.0 0.0.0.255 131.108.200.0 0.0.0.255
end
```

Example 4-20 displays the working configuration of R2, with lines numbered from 1 through 29.

Example 4-20 *R2's Full Configuration*

```
Version 12.2
hostname R2
enable password cisco
crypto isakmp policy 1
hash md5
authentication pre-share
crypto isakmp key CCIe address 131.108.255.1
crypto ipsec transform-set anyname esp-des esp-sha-hmac
mode tunnel
crypto map anyname1 1 ipsec-isakmp
set peer 131.108.255.1
set security-association lifetime seconds 180
set transform-set anyname
match address 100
interface Ethernet0/0
ip address 131.108.200.1 255.255.255.0
interface Serial0/0
 ip address 131.108.255.2 255.255.255.252
 encapsulation frame-relay
 ip split-horizon
 ip ospf network point-to-point
 frame-relay map ip 131.108.255.1 201 broadcast
 frame-relay interface-dlci 201
 frame-relay lmi-type ansi
 crypto map anyname1
 router ospf 1
 network 131.108.0.0 0.0.255.255 area 0
 access-list 100 permit ip 131.108.200.0 0.0.0.255 131.108.100.0 0.0.0.255
end
```

The following debug output is seen on R1 after the network administrator pings remote network 131.108.100.1 from Router R2's console port.

1. Why will the IPSec tunnel not negotiate properly?

```
R2#debug crypto engine
Crypto Engine debugging is on
R2#ping
Protocol [ip]:
Target IP address: 131.108.100.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 131.108.200.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 131.108.100.1, timeout is 2 seconds:
22:58:55: CryptoEngine0: generate alg parameter
22:58:55: CRYPTO_ENGINE: Dh phase 1 status: 0
22:58:55: CRYPTO_ENGINE: Dh phase 1 status: 0
22:58:55: CryptoEngine0: generate alg parameter
22:58:55: CryptoEngine0: create ISAKMP SKEYID for conn id 1
22:58:55: CryptoEngine0: generate hmac context for conn id 1.
22:58:55: %CRYPTO-4-IKMP_BAD_MESSAGE: IKE message from 131.108.255.1   failed it
s sanity check or is malformed....
Success rate is 0 percent (0/5)
R2#
```

2. What subnets will be encrypted between Routers R1 and R2?

3. What IOS command produced the following display and from which router?

```
Crypto Map "anyname1" 1 ipsec-isakmp
        Peer = 131.108.255.2
        Extended IP access list 100
    access-list 100 permit ip 131.108.100.0 0.0.0.255 131.108.200.0 0.0.0.255
        Current peer: 131.108.255.2
        Security association lifetime: 4608000 kilobytes/180 seconds
        PFS (Y/N): N
        Transform sets={ anyname, }
        Interfaces using crypto map anyname1:
                Serial0/0
```

4. Will Host A be able to communicate with Host B or Host C? The following displays are the IP routing tables on R1 and R2. (Assume the gateway configurations on the PCs are correct.)

   R1's IP routing table:

```
R1>show ip route
Codes: C - connected, , O - OSPF,
     131.108.0.0/16 is variably subnetted, 4 subnets, 2 masks
C       131.108.255.0/30 is directly connected, Serial0/0
O       131.108.200.0/24 [110/400] via 131.108.255.2, 00:52:00, Serial0/0
C       131.108.101.0/24 is directly connected, Ethernet0/1
C       131.108.100.0/24 is directly connected, Ethernet0/0
```

   R2's IP routing table:

```
R2>show ip route
Codes: C - connected, , O - OSPF
     131.108.0.0/16 is variably subnetted, 4 subnets, 2 masks
C       131.108.255.0/30 is directly connected, Serial0/0
C       131.108.200.0/24 is directly connected, Ethernet0/0
O       131.108.101.0/24 [110/58] via 131.108.255.1, 00:52:09, Serial0/0
131.108.100.0/24 [110/58] via 131.108.255.1, 00:52:09, Serial0/0
```

5. To allow the IP subnet 131.108.101.0/24 attached to the R1 Ethernet 0/1 interface to be encrypted over the IPSec tunnel and to communicate with the remote PC IP address 131.108.200.5, what configuration changes are required on which router?

Scenario Answers

Scenario Solutions

1. The following debug output advises the network administrator of the problem:

```
22:58:55: %CRYPTO-4-IKMP_BAD_MESSAGE: IKE message from 131.108.255.1   failed it
s sanity check or is malformed....
```

During the IKE negotiation, the router reports a message that identifies the fault as the share password. R2 is configured with the password, CCIe (should match R1's preshared password set to CCIE). See Example 4-17, and code line 7.

Changing the IKE password to CCIE with the IOS command **crypto isakmp key CCIE address 131.108.255.1**, the following debug output confirms the IPSec connections by pinging from R2 Ethernet 0/0 IP address to R1 Ethernet 0/0 IP address:

```
R2#ping
Protocol [ip]:
Target IP address: 131.108.100.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 131.108.200.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 131.108.100.1, timeout is 2 seconds:
23:12:21: CryptoEngine0: generate alg parameter
23:12:21: CRYPTO_ENGINE: Dh phase 1 status: 0
23:12:21: CRYPTO_ENGINE: Dh phase 1 status: 0
23:12:21: CryptoEngine0: generate alg parameter
23:12:21: CryptoEngine0: create ISAKMP SKEYID for conn id 1
23:12:21: CryptoEngine0: generate hmac context for conn id 1
23:12:21: CryptoEngine0: generate hmac context for conn id 1
23:12:21: CryptoEngine0: generate hmac context for conn id 1
23:12:21: CryptoEngine0: clear dh number for conn id 1
23:12:22: CryptoEngine0: generate hmac context for conn id 1
23:12:22: validate proposal 0
23:12:22: validate proposal request 0
23:12:22: CryptoEngine0: generate hmac context for conn id 1.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 12/13/16 ms
R2#
```

The first ping packet fails because the IPSec tunnel has not yet been created. Then, the IPSec tunnel is successfully brought up between R1 and R2.

2. Access-list 100 on both routers defines the IP subnets that need to be encrypted between R1 and R2. Packets flowing between subnets 131.108.100.0/24 and 131.108.200.0/24 will be encrypted.

   R1's ACL is as follows:

   ```
   access-list 100 permit ip 131.108.100.0 0.0.0.255 131.108.200.0 0.0.0.255
   ```

   R2's ACL is as follows:

   ```
   access-list 100 permit ip 131.108.200.0 0.0.0.255 131.108.100.0 0.0.0.255
   ```

3. The **show crypto map** IOS command displays the remote peer address and the transform set. The previous displays are taken from R1 because the remote peer address is displayed as 131.108.255.2 (R2's serial 0/0 IP address).

4. Yes, because IPSec has nothing to do with routing IP data, IPSec will encrypt only data as configured. R1 has a remote entry to the network residing on R2, and R2 has a remote entry to the network residing on R1. Traffic between A and C and B and C will not be encrypted; only traffic between A and B will be encrypted.

   Here is a sample ping request from R2 to R1 and Host A and Host C:

   ```
   R2>ping 131.108.100.1
   Type escape sequence to abort.
   Sending 5, 100-byte ICMP Echos to 131.108.100.1, timeout is 2 seconds:
   !!!!!
   Success rate is 100 percent (5/5), round-trip min/avg/max = 4/6/8 ms
   R2>
   R2>ping 131.108.101.1
   Type escape sequence to abort.
   Sending 5, 100-byte ICMP Echos to 131.108.101.1, timeout is 2 seconds:
   !!!!!
   Success rate is 100 percent (5/5), round-trip min/avg/max = 4/6/8 ms
   R2>
   R2>ping 131.108.100.5
   Type escape sequence to abort.
   Sending 5, 100-byte ICMP Echos to 131.108.100.5, timeout is 2 seconds:
   !!!!!
   Success rate is 100 percent (5/5), round-trip min/avg/max = 4/6/8 ms
   R2>
   R2>ping 131.108.101.5
   Type escape sequence to abort.
   Sending 5, 100-byte ICMP Echos to 131.108.105.1, timeout is 2 seconds:
   !!!!!
   Success rate is 100 percent (5/5), round-trip min/avg/max = 4/6/8 ms
   ```

5. Because the source network is located on R1, access-list 100 on R1 needs to be modified, remembering that, by default, an implicit deny is defined on ACL 100. Network 131.108.101.0/24 is only permitted to encrypt traffic to the static IP address 131.108.200.5, hence the ACL line required on R1 becomes the following:

```
access-list 100 permit ip 131.108.100.5 0.0.0.0 131.108.200.0 0.0.0.255
access-list 100 permit ip 131.108.101.0 0.0.0.255 131.108.200.5 0.0.0.0
```

or:

```
access-list 100 permit ip 131.108.100.5 0.0.0.0 131.108.200.0 0.0.0.255
access-list 100 permit ip 131.108.101.0 0.0.0.255 host 131.108.200.5
```

On R2 the access list becomes:

```
access-list 100 permit ip 131.108.200.0 0.0.0.255 131.108.101.0 0.0.0.255
access-list 100 permit ip 131.108.200.5 0.0.0.0 131.108.100.0 0.0.0.255
```

IP routing is already configured and working. IPSec will ensure only that IP data is encrypted.