CHAPTER 14

GRE Tunneling over IPsec

Generic routing encapsulation (GRE) tunnels have been around for quite some time. GRE was first developed by Cisco as a means to carry other routed protocols across a predominantly IP network. Some network administrators tried to reduce the administrative overhead in the core of their networks by removing all protocols except IP as a transport. As such, non-IP protocols such as IPX and AppleTalk were tunneled through the IP core via GRE.

GRE adds a new GRE header to the existing packet. This concept is similar to IPsec tunnel mode. The original packet is carried through the IP network, and only the new outer header is used for forwarding. Once the GRE packet reaches the end of the GRE tunnel, the external header is removed, and the internal packet is again exposed.

Today, multiprotocol networks have mostly disappeared. It is difficult to find traces of the various protocols that used to be abundant throughout enterprise and core infrastructures. In a pure IP network, GRE was initially seen as a useless legacy protocol. But the growth of IPsec saw a rebirth in the use of GRE in IP networks. This chapter talks about the use of GRE in an IPsec environment.

"Do I Know This Already?" Quiz

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

The 15-question quiz, derived from the major sections in the "Foundation Topics" portion of the chapter, helps you to determine how to spend your limited study time.

Table 14-1 outlines the major topics discussed in this chapter and the "Do I Know This Already?" quiz questions that correspond to those topics.

Table 14-1 *"Do I Know This Already?" Foundation Topics Section-to-Question Mapping*

Foundation Topics Section	Questions Covered in This Section	Score
GRE Characteristics	1	
GRE Header	2	
Basic GRE Configuration	3	
Secure GRE Tunnels	4–5	
Configure GRE over IPsec Using SDM	6–15	
Total Score		

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

1. What is the minimum amount of additional header that GRE adds to a packet?
   a. 16 bytes
   b. 20 bytes
   c. 24 bytes
   d. 36 bytes
   e. 48 bytes
2. Which of the following are valid options in a GRE header (select all that apply)?
   a. GRE Header Length
   b. Checksum Present
   c. Key Present
   d. External Encryption
   e. Protocol
3. What is the purpose of a GRE tunnel interface?
   a. It is always the tunnel source interface.
   b. It is always the tunnel destination interface.
   c. It is where the protocol that travels through the tunnel is configured.
   d. It is the interface that maps to the physical tunnel port.
   e. It is not used today.

4. When IPSec transport mode is used, how many IP headers are found in the GRE over IPsec packet?
   a. One—the original IP header is replicated when needed.
   b. Two—the original IP header and the GRE IP header.
   c. Two—the original IP header and the IPsec IP header.
   d. Three—the original IP header, the GRE IP header, and the IPsec IP header.
   e. Four—the original IP header, the GRE IP header, the IPsec IP header, and the outer IP header.
5. What feature does GRE introduce that cannot be accomplished with normal IPsec?
   a. GRE increases the packet size so that the minimum packet size is easily met.
   b. GRE adds robust encryption to protect the inner packet.
   c. GRE requires packet sequencing so that out-of-order packets can be reassembled correctly.
   d. GRE adds an additional IP header to further confuse packet-snooping devices.
   e. GRE permits dynamic routing between end sites.
6. What are the basic components within the Secure GRE Wizard (select all that apply)?
   a. Router interface configuration
   b. GRE tunnel configuration
   c. IPsec parameters configuration
   d. Router authentication configuration
   e. Routing protocols configuration
7. What is the IP address inside of the GRE tunnel used for?
   a. The GRE tunnel peering point.
   b. The IPsec tunnel peering point.
   c. The routing protocols peering point.
   d. The management interface of the router.
   e. There is no IP address inside of the GRE tunnel.
8. Which option must be configured if a backup secure GRE tunnel is configured?
   a. Source interface
   b. Source IP address
   c. Destination interface
   d. Destination IP address
   e. Destination router name

9. What methods are available for VPN authentication when used with a GRE tunnel (select all that apply)?
   a. Digital certificates
   b. Pre-shared keys
   c. Biometrics
   d. OTP
   e. KMA
10. When creating/selecting an IKE proposal, what does the Priority number indicate?
   a. The Priority number is a sequence number.
   b. The Priority number determines the encryption algorithm.
   c. The Priority number helps determine the authentication method.
   d. The Priority number is related to the Diffie-Hellman group.
   e. The Priority number is necessary to select the hash algorithm.
11. How are IPsec transform sets used in the Secure GRE Wizard?
   a. There must be a unique IPsec transform set for each VPN peer.
   b. There must be a unique IPsec transform set for each GRE tunnel.
   c. The two ends of a VPN must use the same IPsec transform set.
   d. The same IPsec transform set can be used for all VPN peers.
   e. Site-to-site IPsec VPN transform sets cannot be used for GRE over IPsec VPNs.
12. Which dynamic routing protocols can be configured in the GRE over IPsec tunnel (select all that apply)?
   a. RIP
   b. OSPF
   c. EIGRP
   d. BGP
   e. Static
13. Which routing options are appropriate when using both a primary and a backup GRE tunnel (select all that apply)?
   a. RIP
   b. OSPF
   c. EIGRP
   d. BGP
   e. Static

14. When using OSPF in the GRE over IPsec tunnel, what OSPF parameters must match so that the two peers establish an OSPF adjacency (select all that apply)?

    a. IP address of the GRE tunnel interface

    b. Subnet of the GRE tunnel interface

    c. OSPF area of the GRE tunnel interface

    d. OSPF process ID of each router

    e. Number of networks configured in OSPF on each router

15. In the Summary of the Configuration window, how can the displayed configuration be modified?

    a. Type changes directly into the scroll window and click the **Apply** button at the bottom of the window.

    b. Changes cannot be made from within any wizard.

    c. Click the **Modify** button to return to the configuration windows.

    d. Click the **Back** button to return to the configuration windows.

    e. Click the **Next** button to proceed to the Modify Configuration window.

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

- **10 or fewer overall score**—Read the entire chapter. This includes the "Foundation Topics," "Foundation Summary," and "Q&A" sections.

- **11 or 13 overall score**—Begin with the "Foundation Summary" section, and then go to the "Q&A" section.

- **14 or more overall score**—If you want more review on these topics, skip to the "Foundation Summary" section, and then go to the "Q&A" section. Otherwise, move to the next chapter.

Foundation Topics

GRE Characteristics

The initial power of GRE was that anything could be encapsulated into it. The primary use of GRE was to carry non-IP packets through an IP network; however, GRE was also used to carry IP packets through an IP cloud. Used this way, the original IP header is buried inside of the GRE header and hidden from prying eyes. The generic characteristics of a GRE tunnel are as follows:

- A GRE tunnel is similar to an IPsec tunnel because the original packet is wrapped inside of an outer shell.
- GRE is stateless, and offers no flow control mechanisms.
- GRE adds at least 24 bytes of overhead, including the new 20-byte IP header.
- GRE is multiprotocol and can tunnel any OSI Layer 3 protocol.
- GRE permits routing protocols to travel through the tunnel.
- GRE was needed to carry IP multicast traffic until Cisco IOS Software Release 12.4(4)T.
- GRE has relatively weak security features.

The GRE tunnel itself is similar to an IPsec tunnel. The tunnel has two endpoints. Traffic enters one end of the tunnel and exits the other end. While in the tunnel, routers use the new outer header only to forward the packets.

The GRE tunnel is stateless. Unlike an IPsec tunnel, the endpoints do not coordinate any parameters before sending traffic through the tunnel. As long as the tunnel destination is routable, traffic can flow through it. Also, by default, GRE provides no reliability or sequencing. Such features are typically handled by upper-layer protocols.

GRE tunnels offer minimal security, whereas IPsec offers security by means of confidentiality, data authentication, and integrity assurance. GRE has a basic encryption mechanism, but the key is carried along with the packet, which somewhat defeats the purpose.

GRE does add an additional 24-byte header of overhead. This overhead contains a new 20-byte IP header, which indicates the source and destination IP addresses of the GRE tunnel. The remaining 4 bytes are the GRE header itself. Additional GRE options can increase the GRE header by up to another 12 bytes.

It is important to note that the larger packet size caused by the additional headers can have a detrimental effect on network performance. Because the additional headers are dynamically added, most users believe that nothing "bad" can happen as a result. If a packet is larger than the interface maximum transmission unit (MTU) permits, the router must fragment the packet into smaller pieces to fit. This fragmentation effort can add significant CPU overhead to a router, which can affect all packet forwarding.

GRE is a simple yet powerful tunneling tool. It can tunnel any OSI Layer 3 protocol over IP. As such, it is basically a point-to-point private connection. A private connection between two endpoints is the basic definition of a VPN.

Unlike IPsec, GRE permits routing protocols (such as OSPF and EIGRP) across the connection. This is not the case with typical IPsec tunnels. IPsec tunnels can send IP packets, but not routing protocols. Before the IP packets can travel through the IPsec tunnel, however, static routes are necessary on each IPsec endpoint for routing awareness of the opposite end. This additional configuration overhead does not scale well with a large number of IPsec tunnels.

Until Cisco IOS Software Release 12.4(4)T, IP multicast had to be sent over GRE. Prior to this IOS release, IPsec could not carry IP multicast traffic. Even though IOS 12.4(4)T now supports IP multicast traffic, GRE over IPsec still must be used to carry dynamic routing protocols.

GRE does not have any strong security features. The header provides an optional, albeit weak, security key mechanism. As a result, no strong confidentiality, data source authentication, or data integrity mechanisms exist in GRE. However, IPsec provides confidentiality (DES, 3DES, or AES), and source authentication and data integrity with MD5 or SHA-1 HMACs.

Thus, a GRE tunnel, which carries multicast and routing traffic, can be sent through an IPsec tunnel for enhanced security.

GRE Header

The GRE header itself contains 4 bytes, which represent the minimum size of GRE header with no added options. The first pair of bytes (bits 0 through 15) contains the flags that indicate the presence of GRE options. Such options, if active, add additional overhead to the GRE header. The second pair of bytes is the protocol field and indicates the type of data that is carried in the GRE tunnel. Table 14-2 describes the GRE header options.

Table 14-2 *GRE Header Options*

GRE Header Bit	Option	Description
0	Checksum Present	Adds a 4-byte checksum field to the GRE header after the protocol field if this bit is set to 1.
2	Key Present	Adds a 4-byte encryption key to the GRE header after the checksum field if this bit is set to 1.
3	Sequence Number Present	Adds a 4-byte sequence number to the GRE header after the key field if this bit is set to 1.
13–15	GRE Version	0 indicates basic GRE, while 1 is used for PPTP.

The Checksum Present option (bit 0) adds an optional 4-byte checksum field to the GRE header. This checksum appears after the protocol field in the GRE header only if the Checksum Present bit is set. Normally, this option is not needed because other upper-layer protocols provide checksum capabilities to detect packet corruption.

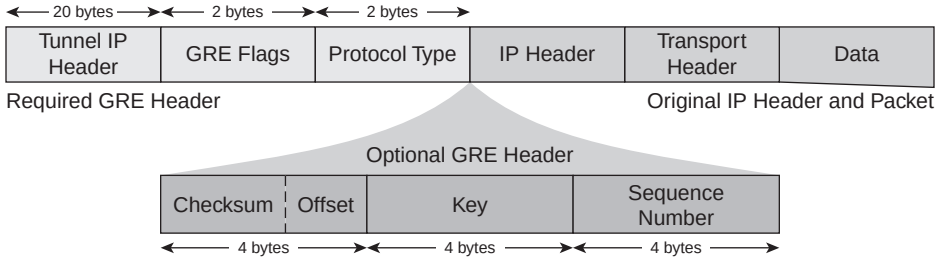
The Key Present option (bit 2) adds an optional 4-byte key field to the GRE header. This clear-text key follows the checksum field. The key is used to provide basic authentication where each GRE endpoint has the key. However, the key itself is exposed in the GRE header. Due to this vulnerability, GRE encryption is not typically used. However, the key value can be used to uniquely identify multiple tunnels between two endpoints. This would be similar to an IPsec SPI.

The Sequence Number option (bit 3) adds an optional 4-byte sequence number field to the GRE header. This sequence value follows the key option. This option is used to properly sequence GRE packets upon arrival. Similar to the checksum option, this is not typically used because upper-layer protocols also offer this functionality.

Bits 13–15 indicate the GRE version number. 0 represents basic GRE, while 1 shows that the Point-to-Point Tunneling Protocol (PPTP) is used. PPTP is not covered in this book.

The second 2 bytes of the GRE header represent the Protocol field. These 16 bits identify the type of packet that is carried inside the GRE tunnel. Ethertype 0x0800 indicates IP. Figure 14-1 shows a GRE packet with all options present added to an IP header and data.

Figure 14-1 *GRE Packet Format*

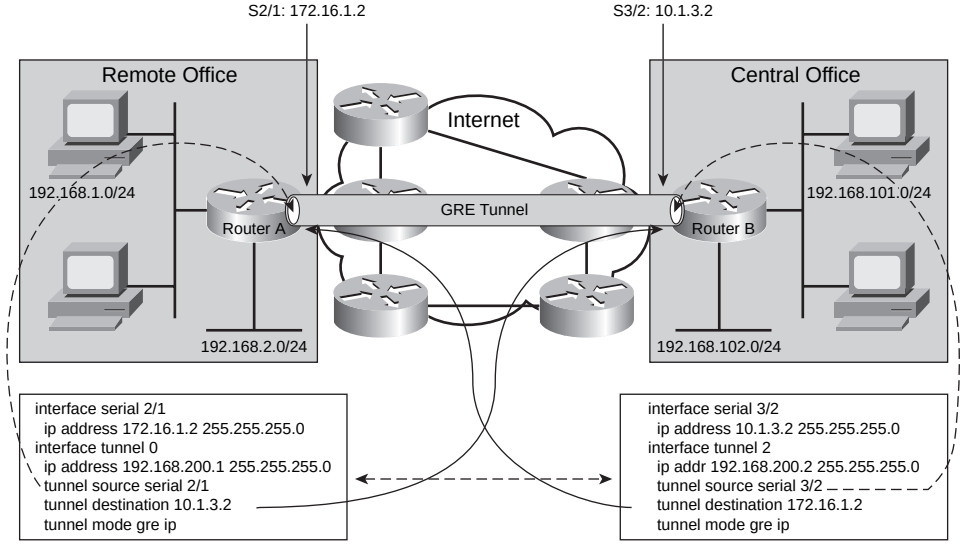


In Figure 14-1, only the required GRE header and original IP header and packet typically appear in GRE tunnel configurations. The GRE options are normally not used because upper-layer protocols provide similar functionality.

Basic GRE Configuration

A GRE tunnel carries some Layer 3 protocol between two IP endpoints. During the initial use of GRE tunnels, the tunnel contents were typically any protocol except IP. Today, GRE tunnels are used to carry IP data over an IP network. But the GRE tunnel itself can be sent through an IPsec tunnel for security. Figure 14-2 shows a basic GRE tunnel setup.

Figure 14-2 *GRE Tunnel Configuration*



The basic configuration components of a GRE tunnel include

- A tunnel source (an interface or IP address local to this router)
- A tunnel destination (an IP address of a remote router)
- A tunnel mode (GRE/IP is the default)
- Tunnel traffic (data that travels through the tunnel, and is encapsulated by the GRE header)

In Figure 14-2, two IP endpoints have a GRE tunnel configured between them. The GRE tunnel is actually defined as an interface in each router. The GRE interface is what makes GRE multiprotocol. IPsec crypto maps can match only IP access lists. A router interface can be configured for, and thus transport, any protocol. The available protocols are dependent upon the Cisco IOS feature set installed.

TIP The Cisco Software Advisor (http://tools.cisco.com/Support/Fusion/FusionHome.do) helps select the appropriate IOS feature set for any given Cisco router platform.

The tunnel source and destination are IP interfaces. Thus, the GRE travels across an IP network. The protocol configured on the GRE interfaces is the data that travels through the GRE tunnel.

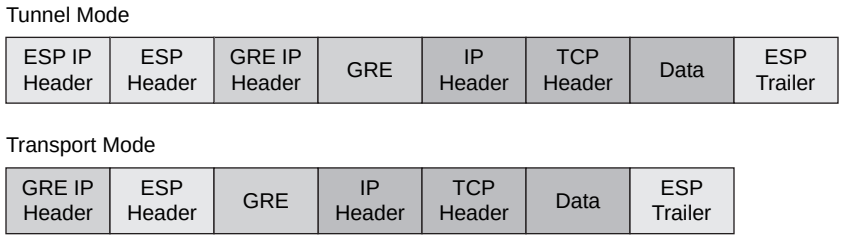
The GRE tunnel source on one end must match the destination on the other end, and vice versa. This IP validation is performed as the GRE tunnel is established. For proper routing through the GRE tunnel, a common subnet should be configured within the tunnel.

In Figure 14-2, IP is configured within the GRE tunnel. The two sites, as well as the tunnel itself, use RFC 1918 private addressing. IP routing flows between the sites through the GRE tunnel by means of your favorite routing protocol (not shown). For documentation purposes, the public network also uses private addressing, although this certainly is not a requirement.

Secure GRE Tunnels

"GRE over IPsec" implies that the GRE packet sits higher in the stack than the IPsec portion. Similar to how TCP/IP is represented, TCP is at Layer 4, while IP is at Layer 3. When laid out in a graphical packet, the TCP portion is inside of the IP part. The same is true with GRE over IPsec. The original packet is the innermost layer. Then the GRE wrapper appears. Finally, the IPsec portion is added for security. Figure 14-3 shows the GRE over IPsec packet format.

Figure 14-3 *GRE over IPsec Packet Format*



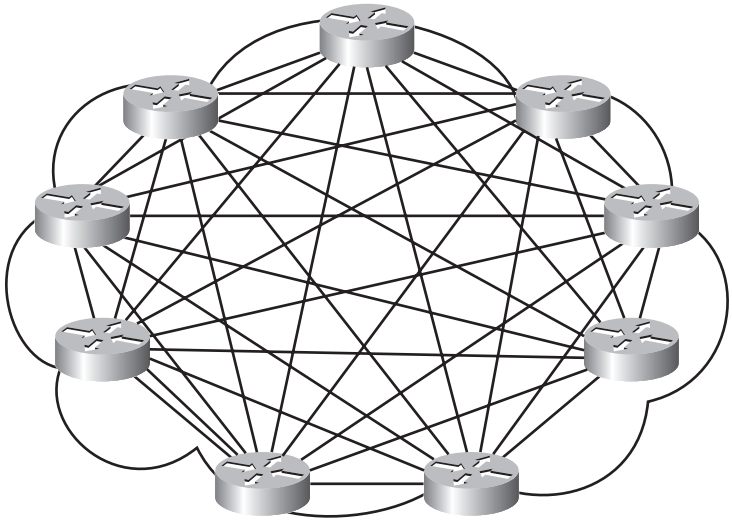
As Figure 14-3 shows, there are multiple IP layers in a GRE over IPsec packet. The innermost layer is the original IP packet. This represents data that is traveling between two devices, or two sites. The initial IP packet is wrapped in a GRE header to permit routing protocols to travel between in the GRE tunnel (something that IPsec alone cannot do). And IPsec is added as the outer layer to provide confidentiality and integrity (which is a shortcoming of GRE by itself). The end result is that two sites can securely exchange routing information and IP packets.

Figure 14-3 is also a reminder of the two IPsec modes: tunnel and transport. Transport mode is used if the original IP header can be exposed, while tunnel mode protects the original IP header within a new IPsec IP header. When using GRE over IPsec, transport mode is often sufficient, because the GRE and IPsec endpoints are often the same. Whether tunnel or transport mode is selected, the original IP header and packet are fully protected.

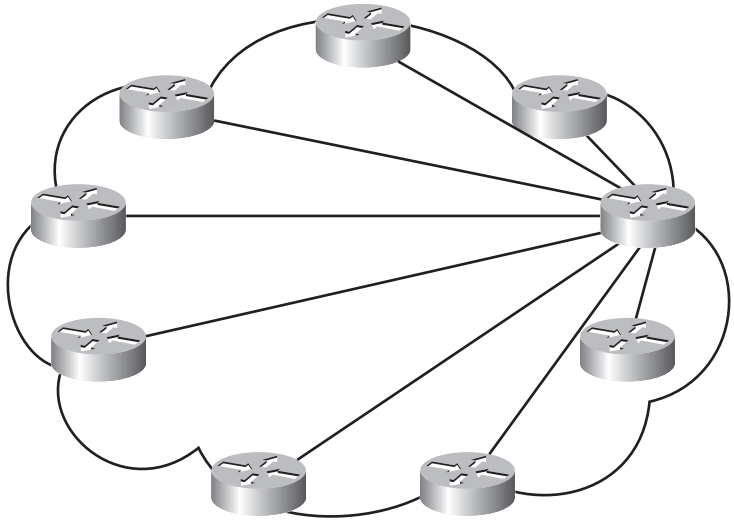
What might get lost in Figure 14-3 is the size of the new packets created due to the additional encapsulations. Each IP header adds 20 bytes to the packet size. This does not include overhead for ESP and GRE headers. For small IP packets, it is possible that the GRE over IPsec headers may be much larger than the original packet itself. Network efficiency can be determined by the ratio of actual data compared to the overhead associated with transporting the data. When there is more overhead (packet headers) than actual data, then the network is inherently less efficient.

Most GRE over IPsec implementations use a hub-and-spoke design. Although not a requirement, such a design minimizes the management overhead seen with managing a large number of IPsec tunnels. For example, if ten sites were fully meshed with GRE over IPsec tunnels, it would take 45 tunnels ([10 * 9]/2). In a hub-and-spoke design, full connectivity (via the hub) is accomplished with only nine tunnels. Figure 14-4 graphically compares a full mesh of tunnels versus a hub-and-spoke design.

Figure 14-4 *Full Mesh versus Hub-and-Spoke*



Full Mesh



Hub and Spoke

In a normal IPsec tunnel, static routes are needed to direct IP packets into the IPsec VPN tunnel. Routing protocols can run inside the GRE tunnel, creating a dynamic routing topology. GRE provides the routing connectivity, while IPsec provides the confidentiality and integrity. With GRE, routing protocols can now run inside the IPsec tunnel.

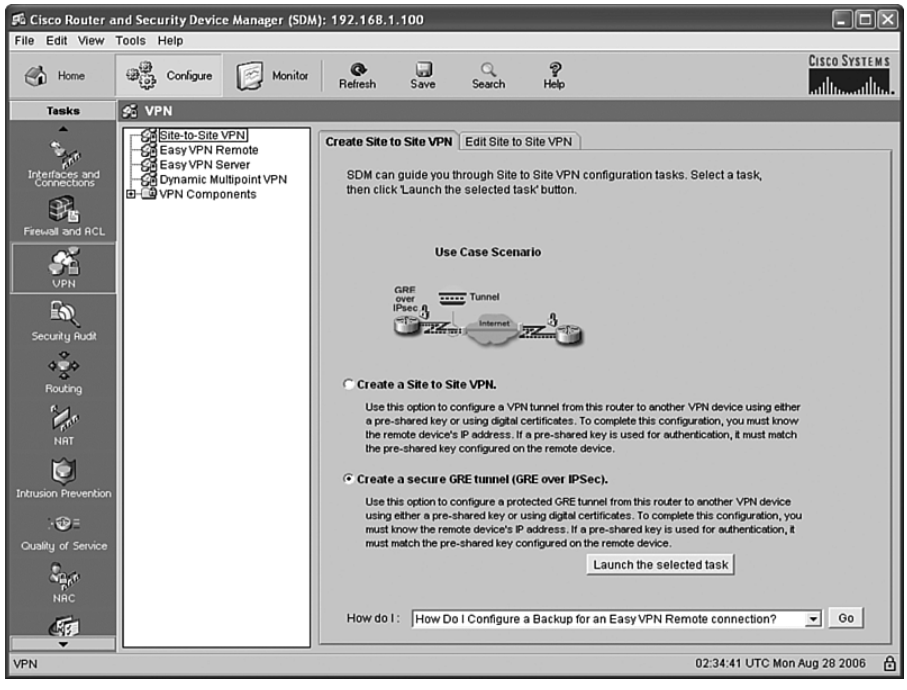
Configure GRE over IPsec Using SDM

This chapter explores how to configure GRE over IPsec using the SDM tool. The previous chapter gave you the opportunity to create an IPsec tunnel in SDM, and get familiar with the SDM interface. This section expands upon previous navigation skills that you have learned.

Launch the GRE over IPsec Wizard

The GRE over IPsec wizard is accessed from the same window that started the Site-to-Site VPN wizard as seen in Chapter 13. Figure 14-5 shows how to access the GRE over IPsec wizard.

Figure 14-5 *GRE over IPsec Wizard*



Similar to how the Site-to-Site VPN Wizard was initiated in Chapter 13, the GRE over IPsec wizard is accessed as follows:

Step 1 Click the **Configure** button at the top of the window.

Step 2 Click the **VPN** button in the Tasks bar on the left.

Step 3 Click the **Site-to-Site VPN** option at the top of the menu.

Step 4 Click the **Create Site to Site VPN** tab in the window.

Step 5 Click the **Create a secure GRE tunnel (GRE over IPSec)** radio button.

Step 6 Click the **Launch the selected task** button at the bottom of the window.

When you successfully accomplish these tasks, the Secure GRE Wizard starts. The Secure GRE Tunnel (GRE over IPsec) window reminds you of the capabilities and purpose of such a tunnel. The basic steps of the Secure GRE Wizard are as follows:

Step 1 Create the GRE tunnel.

Step 2 Create a backup GRE tunnel (optional).

Step 3 Select the IPsec VPN authentication method.

Step 4 Select the IPsec VPN IKE proposals.

Step 5 Select the IPsec VPN transform sets.

Step 6 Select the routing method for the GRE over IPsec tunnel.

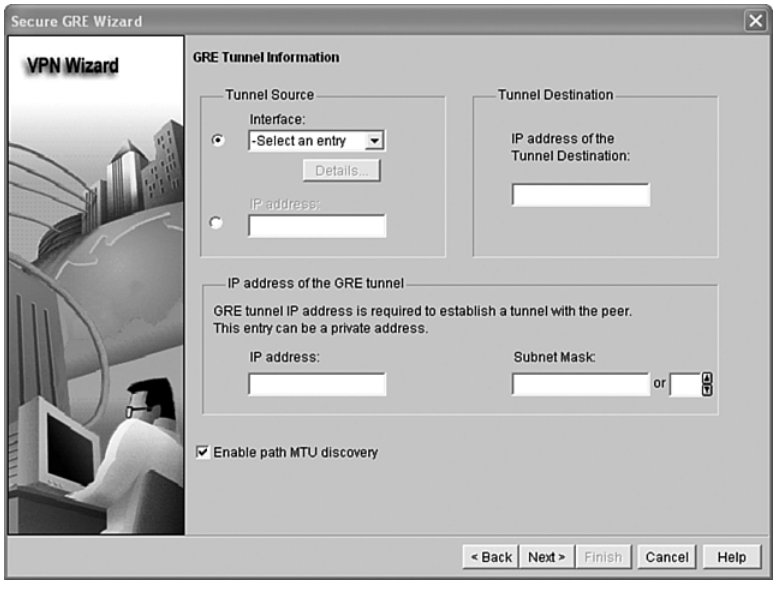
Step 7 Validate the GRE over IPsec configuration.

To continue into the wizard, click **Next>** at the bottom of the window.

Step 1: Create the GRE Tunnel

The first part of the GRE over IPsec tunnel is the GRE tunnel. Figure 14-3 showed the various layers within the GRE over IPsec tunnel. The original IP packet is the innermost portion. Next comes the GRE layer. Figure 14-6 shows the GRE Tunnel Information window.

Figure 14-6 *GRE Tunnel Information*



The GRE Tunnel Information window is the first configuration window of the Secure GRE Wizard. There are two sets of IP addresses that are applied to the GRE tunnel interface—the tunnel source and destination (at the top of the window) represent the GRE IP header (shown in Figure 14-3).

The tunnel source is either selected from a pull-down list of interfaces in this router or entered manually. If an interface is selected from the list, the IP address of the interface is automatically used as the GRE tunnel source. The tunnel destination is the IP address of the remote GRE peer and must be manually entered.

The IP address of the GRE tunnel is the IP subnet used within the tunnel itself. This subnet can be used for management (the other end can be pinged) or, more importantly, for routing protocol neighbors. The remote GRE peer must use a unique IP address on the same inner subnet.

Path MTU is enabled by default. Remember that GRE over IPsec considerably increases the IP packet size. Path MTU discovery uses Internet Control Message Protocol (ICMP) Unreachable messages to determine the maximum packet size possible between the GRE peers. If needed, fragmentation can then be performed by the GRE endpoints, versus en route, where it might not be performed at all.

When you are finished with the GRE Tunnel Information window, click **Next>** at the bottom of the window.

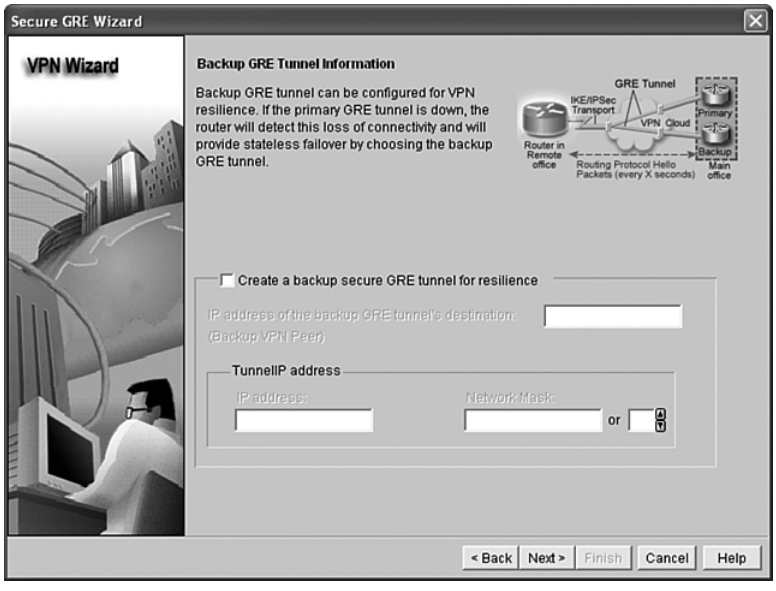
Step 2: Create a Backup GRE Tunnel

The Secure GRE Wizard offers the option to create a second GRE tunnel for survivability. If the GRE tunnel fails for any reason, then the IPsec tunnel that is carried within it fails also. A backup GRE tunnel provides stateless failover in the event of the loss of the primary GRE tunnel. Figure 14-7 shows the Backup GRE Tunnel Information window.

Because a backup GRE tunnel is an optional feature, you must check the **Create a backup secure GRE tunnel for resilience** box to activate this window. Once checked, the configuration options are very similar to those used to create the primary GRE tunnel.

The same tunnel source is used for both the primary and backup GRE tunnels, so there is no opportunity to select a tunnel source in the Backup window. Either an interface or a local IP address was entered earlier for the primary GRE tunnel. Simply enter the IP address of the alternate peer for this backup GRE tunnel. This IP address could be a different interface on the same peer router, or an entirely different device at the remote site.

Figure 14-7 *Backup GRE Tunnel Information*



Similar to the primary GRE tunnel, you must create a unique IP address on a new IP subnet within this backup tunnel. The remote peer must use the same subnet with an exclusive IP address of its own. As with the primary GRE tunnel, the inner IP addresses are used to establish routing protocol neighbors.

When you are finished with the Backup GRE Tunnel Information window, click **Next>** at the bottom of the window.

Steps 3–5: IPsec VPN Information

The outermost layer of the GRE over IPsec tunnel is the IPsec VPN. The various windows used to enter the IPsec information are nearly identical to those used to create a site-to-site IPsec VPN discussed in Chapter 13, “Site-to-Site VPN Operations.”

The first IPsec VPN task is to enter the VPN authentication information. Similar to Figure 13-14, either digital certificates or pre-shared keys can be used. If pre-shared keys are selected, the key must be entered twice to ensure accuracy.

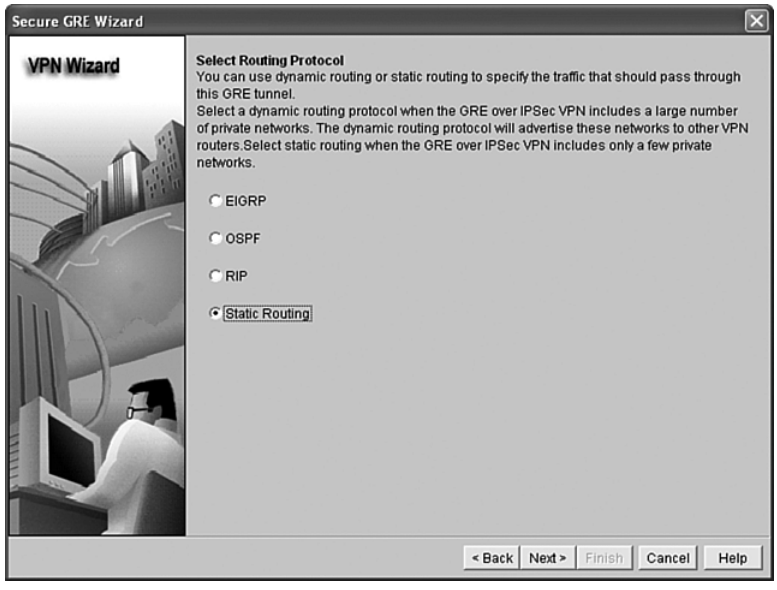
The second IPsec VPN task is to select or create IKE proposals. This window is identical to the one shown in Figure 13-15, as are the procedures used to select an appropriate IKE proposal for this IPsec VPN. Remember that the remote IPsec peer must have an identical IKE proposal configured, and that the same IKE proposal can be used for many remote peers.

The third IPsec VPN task is to select or create IPsec transform sets. This window is identical to the one shown in Figure 13-16. From here, new transform sets can be created, and the appropriate transform set can be selected for use with this IPsec VPN. Remember that the remote IPsec peer must have an identical IPSec transform set configured, and that the same IPsec transform set can be used for many remote peers.

Step 6: Routing Information

Once both the GRE tunnel and the IPsec tunnels have been configured, the final step is to select a routing protocol to traverse the GRE tunnel. Remember that with a typical IPsec VPN, the only routing option is to configure static routes on each side. These static routes manually determine which prefixes are reachable through the IPsec VPN. Figure 14-8 shows the Select Routing Protocol window of the Secure GRE Wizard.

Figure 14-8 *Select Routing Protocol*



Static Routing is the default option (radio button) in the routing protocol selection process. There are four routing options supported within the GRE tunnel:

- EIGRP
- OSPF
- RIP
- Static routing

Each routing option uses the Routing Information window to configure individual options. Routes that are manually configured (static) or dynamically exchanged (RIP, OSPF, or EIGRP) through the GRE over IPsec tunnel become the "interesting traffic" described that decides which traffic is encrypted through the IPsec tunnel. Once you have selected a routing protocol, click **Next>** at the bottom of the window to proceed to the Routing Information window for the appropriate routing protocol.

When using the GRE over IPsec wizard, RIP is not an available dynamic routing option from the Select Routing Protocol window if a backup GRE tunnel was configured earlier. Only OSPF or EIGRP can be enabled when two GRE tunnels to the same remote location are used.

Static Routes

Static routing is typically used to support small stub sites that only have a single subnet. No dynamic routing information is exchanged between sites. If a site has multiple subnets that are to use the VPN, or if a site uses backup VPN tunnels, then static routing is inappropriate.

If static routing is selected in the Select Routing Protocol window of the wizard, the first choice presented is whether to do split tunneling or not. Split tunneling allows the router to send some traffic through the IPsec VPN to the remote side, and the remainder of the traffic unprotected into the public network. This is very similar to the definition of interesting traffic with IPsec VPNs. Enter an IP subnet and subnet mask that is to be protected in the VPN tunnel.

The wizard permits only a single static route to be configured within the split tunneling option. If split tunneling is not selected (the Tunnel All Traffic option), then a default route is added to the router that sends all traffic through the GRE over IPsec tunnel.

When you are finished with the static routing options, click **Next>** at the bottom of the window to advance to the Summary of the Configuration window.

RIP

The first RIP configuration option is the version. Select version 1 to use the older classful version of RIP, or version 2 for the more modern classless version that sends the subnet mask with the routing updates. Next, click the **Add...** button local networks to the RIP routing protocol. Remember that you can add only whole classful network numbers to RIP, and all subnets of that network number are included. You must add the IP subnet of the GRE interface for RIP to use the interface.

Routes that are not added to the RIP configuration are not exchanged through the GRE over IPsec tunnel. Only traffic in the exchanged routes is protected by the VPN. Traffic outside of the RIP

routes avoids the VPN. It is important that the remote router also correctly configure RIP so routing neighbors can be formed.

When you are finished with the RIP options, click **Next>** at the bottom of the window to advance to the Summary of the Configuration window.

OSPF

The first OSPF task is to select or create an OSPF process ID. If OSPF is already operational in the router, you can select a process ID from the pull-down menu. If not, you must create a new OSPF process in the router. Once the process ID is configured, you must determine the OSPF area ID to be used in the GRE over IPsec tunnel.

Next, you must click the **Add...** button to add local networks to the OSPF routing protocol. In OSPF, you must enter a subnet number, a wildcard mask, and an area for each network. You must add the IP subnet/mask/area of the GRE interface for OSPF to use the interface.

Routes that are not added to the OSPF configuration are not exchanged through the GRE over IPsec tunnel. Only traffic in the exchanged routes is protected by the VPN. Traffic outside of the OSPF routes avoids the VPN. It is important that the remote router also correctly configure OSPF so routing adjacencies can be formed. For OSPF, this means that both peers use a common subnet and the same OSPF area.

When you are finished with the OSPF options, click **Next>** at the bottom of the window to advance to the Summary of the Configuration window.

EIGRP

The first EIGRP task is to select or create an EIGRP autonomous system (AS) number. If EIGRP is already operational in the router, you can select an AS number from the pull-down menu. If not, you must create a new EIGRP AS number in the router.

Then, you must click the **Add...** button to add local networks to the EIGRP routing protocol. In EIGRP, you must enter a subnet number and a wildcard mask for each network. You must add the IP subnet/mask of the GRE interface for EIGRP to use the interface.

Routes that are not added to the EIGRP configuration are not exchanged through the GRE over IPsec tunnel. Only traffic in the exchanged routes is protected by the VPN. Traffic outside of the EIGRP routes avoids the VPN. It is important that the remote router also correctly configure EIGRP so routing neighbors can be formed. For EIGRP, this means that both peers use a common subnet and the same EIGRP AS.

When you are finished with the EIGRP options, click **Next>** at the bottom of the window to advance to the Summary of the Configuration window.

Step 7: Validate the GRE over IPsec Configuration

Once you advance beyond either of the routing options (the appropriate Routing Information window), you reach the Summary of the Configuration window. You likely need to use the scrollbar to view the entire configuration created by the Secure GRE Wizard. This window is identical to the summary window at the end of the Site-to-Site VPN Wizard. The differences here are the additional configuration options of the GRE tunnel and the routing protocol (if one was configured).

As with the Site-to-Site VPN Wizard, you can either click Finish to end the wizard from this window or click **<Back** to go back into the wizard to modify any of the configurations shown.

Once the configuration is complete, the procedures to test and monitor the GRE over IPsec tunnel are identical to those for the site-to-site IPsec tunnel described in Chapter 13.

Foundation Summary

The generic characteristics of a GRE tunnel are as follows:

- A GRE tunnel is similar to an IPsec tunnel because the original packet is wrapped inside an outer shell.
- GRE is stateless and offers no flow control mechanisms.
- GRE adds at least 24 bytes of overhead, including the new 20-byte IP header.
- GRE is multiprotocol and can tunnel any OSI Layer 3 protocol.
- GRE permits routing protocols to travel through the tunnel.
- GRE was needed to carry IP multicast traffic until 12.4(4)T.
- GRE has relatively weak security features.

Table 14-3 describes the GRE header options.

Table 14-3 *GRE Options*

GRE Header Bit	Option	Description
0	Checksum Present	Adds a 4-byte checksum field to the GRE header after the protocol field if this bit is set to 1.
2	Key Present	Adds a 4-byte encryption key to the GRE header after the checksum field if this bit is set to 1.
3	Sequence Number Present	Adds a 4-byte sequence number to the GRE header after the key field if this bit is set to 1.
13–15	GRE Version	0 indicates basic GRE, while 1 is used for PPTP.

The basic configuration components of a GRE tunnel include

- A tunnel source (an interface or IP address local to this router)
- A tunnel destination (an IP address of a remote router)
- A tunnel mode (GRE/IP is the default)
- Tunnel traffic (data that travels through the tunnel, and is encapsulated by the GRE header)

GRE over IPsec uses the GRE tunnel to carry dynamic IP routing protocols, and uses IPsec to enforce confidentiality and integrity.

GRE over IPsec using tunnel mode has a total of three IP headers in the packet. GRE over IPsec using transport mode has only two IP headers in the packet.

Most GRE over IPsec implementations use a hub-and-spoke design to limit the number of IPsec tunnels required to secure the entire network.

The Secure GRE Wizard is accessed as follows:

Step 1 Click the **Configure** button at the top of the window.

Step 2 Click the **VPN** button in the Tasks bar on the left.

Step 3 Click the **Site-to-Site VPN** option at the top of the menu.

Step 4 Click the **Create Site to Site VPN** tab in the window.

Step 5 Click the **Create a secure GRE tunnel (GRE over IPSec)** radio button.

Step 6 Click the **Launch the selected task** button at the bottom of the window.

The basic steps of the Secure GRE Wizard include

Step 1 Create the GRE tunnel.

Step 2 Create a backup GRE tunnel (optional).

Step 3 Select the IPsec VPN authentication method.

Step 4 Select the IPsec VPN IKE proposals.

Step 5 Select the IPsec VPN transform sets.

Step 6 Select the routing method for the GRE over IPsec tunnel.

Step 7 Validate the GRE over IPsec configuration.

The GRE Tunnel Information window is where the GRE tunnel is configured in SDM. Configuration includes

- Tunnel source (local interface or IP address)
- Tunnel destination (remote IP address)
- Interior tunnel IP address and subnet mask
- Optional MTU path discovery to know if fragmentation must be performed on this router due to the larger packet size created by GRE over IPsec

The Backup GRE Tunnel Information window is where the backup GRE tunnel is configured in SDM. The backup GRE tunnel uses the same source as the primary GRE tunnel. Configuration includes

- Enable the backup tunnel
- Tunnel destination (remote IP address)
- Interior tunnel IP address and subnet mask

The IPsec VPN configuration has three phases, all of which are identical to those found in the site-to-site IPsec VPN configuration process:

1. VPN authentication
2. IKE proposals
3. IPsec transform sets

There are four routing options supported within the GRE tunnel:

- EIGRP
- OSPF
- RIP
- Static routing

Static routing can configure only one subnet and is not appropriate for sites with multiple subnets or for sites using two GRE tunnels.

RIP cannot be configured if a backup GRE tunnel is configured.

Both OSPF and EIGRP use inverse masks when adding subnets to the routing protocol.

Be sure to include the internal IP subnet of the GRE tunnel in the routing protocol configuration so that the configured protocol will use the GRE tunnel interface.

The Configuration Summary window allows you to view the configuration just created with the wizard. You can return to the wizard by clicking the **<Back** button to make changes, or you can finish the wizard by clicking the **Finish** button.

Q&A

The questions and scenarios in this book are designed to be challenging and to make sure that you know the answer. Rather than allowing you to derive the answers from clues hidden inside the questions themselves, the questions challenge your understanding and recall of the subject.

Hopefully, mastering these questions will help you limit the number of exam questions on which you narrow your choices to two options, and then guess.

You can find the answers to these questions in Appendix A. For more practice with exam-like question formats, use the exam engine on the CD-ROM.

1. What type of security features does GRE have natively?
2. What are the three optional headers possible with GRE?
3. What is the GRE encryption typically used for?
4. What is the relationship between the GRE source and destination addresses on the tunnel endpoints?
5. Which IPsec modes can be used with GRE over IPsec?
6. What is the primary driver to deploying GRE over IPsec?
7. What is the sequence to launch the Secure GRE Wizard in SDM?
8. Which options must be configured on the primary GRE tunnel in the Secure GRE Wizard?
9. Which GRE configuration option is not necessary when creating a backup GRE tunnel?
10. What are the three IPsec tasks that are configured in the Secure GRE Wizard?
11. Which routing options are available in the GRE over IPsec configuration?
12. How many static routes can be configured in the Secure GRE Wizard?
13. Which routing protocols must be used if a backup GRE tunnel is deployed?
14. What options are available in the Configuration Summary window?

Exam Topic List

This chapter covers the following topics that you need to master for the CCNP ISCW exam:

- **Sources of Failures**—Describes how to determine the source of a network failure in an IPsec VPN. Knowing where failures could occur can help you plan for quick recovery.
- **Failure Mitigation**—Describes how to avoid a failure, or how best to react when one occurs.
- **Failover Strategies**—Describes how alternative paths are used to continue the flow of data.
- **WAN Backed Up by an IPsec VPN**—Describes how a nonprotected link can use an established VPN to mitigate failure.