LearnSmart

Exam
Manual

CISCO (642-825)
ISCW

Smarter Training

This LearnSmart exam manual covers the most important topics on the Implementing Secure Converged WAN exam (ISCW – 642-825). By studying this manual, you will become familiar with an array of exam-related content, including:

- Basic Teleworker Services
- Frame-Mode MPLS
- Network Security Strategies
- Cisco IOS firewall
- And more!

Give yourself the competitive edge necessary to further your career as an IT professional and purchase this exam manual today!

ISCW LearnSmart
Exam Manual

Copyright © 2011 by PrepLogic, LLC

Product ID: 011263
Production Date: July 19, 2011

All rights reserved. No part of this document shall be stored in a retrieval system or transmitted by any means, electronic, mechanical, photocopying, recording, or otherwise, without written permission from the publisher. No patent liability is assumed with respect to the use of the information contained herein.

Warning and Disclaimer

Every effort has been made to make this document as complete and as accurate as possible, but no warranty or fitness is implied. The publisher and authors assume no responsibility for errors or omissions. The information provided is on an "as is" basis. The authors and the publisher shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this document.

LearnSmart Cloud Classroom, LearnSmart Video Training, Printables, Lecture Series, Quiz Me Series, Awdeeo, PrepLogic and other PrepLogic logos are trademarks or registered trademarks of PrepLogic, LLC. All other trademarks not owned by PrepLogic that appear in the software or on the Web Site (s) are the property of their respective owners.

Volume, Corporate, and Educational Sales

Favorable discounts are offered on all products when ordered in quantity. For more information, please contact us directly:

1-800-418-6789
solutions@learnsmartsystems.com

International Contact Information

International: +1 (813) 769-0920

United Kingdom: (0) 20 8816 8036

Table of Contents

Abstract

The Cisco Certified Network Professional is one of the most well respected certifications in the world. By attaining it, students and candidates signify themselves as extremely accomplished and capable Network Professionals. These four exams, created by Cisco Systems, are extremely difficult and not to be taken lightly. They cover a myriad of topics, in particular - the ISCW (Implementing Secure Wide Area Converged Networks) exam covers all the way to the most detailed analysis of routing packets across wide area network in a complex, adaptable topology. ISCW is multiple choice, simulative, and incorporates test strategies such as "drag and drop" and "hot area" questions to verify a candidate's knowledge.

Before taking this exam, you should be very familiar with both Cisco technology and networking. You must have also attained the Cisco CCNA certification by passing either the one or two part path.

Your Product

This ISCW Exam Manual has been designed from the ground up with you, the student, in mind. It is lean, strong, and specifically targeted toward the candidate. Unlike many other ISCW products, the LearnSmart ISCW Exam Manual does not waste time with excessive explanations. Instead, it is packed full of valuable techniques, priceless information, and brief, but precisely worded, explanations. While we do not recommend using only this product to pass the exam, but rather a combination of LearnSmart Audio Training, Practice Exams, and Video Training, we have designed the product so that it and it alone can be used to pass the exam.

Implement Basic Teleworker Services

Describe Cable (HFC) Technologies

As can be seen in figure 1, the cable system has many components. Starting from the antenna site, where the broadcast signals are received, everything is processed, formatted and distributed at the headend. The signal is sent from the headend over the transportation network using broadband. As the signals proceed farther from the headend, amps are used to boost the signal. The distribution network is used to get the signal in the area of the subscriber. A node converts the optical signal to the RF signal for the feeder lines in the neighborhood. Taps are used to provide multiple outlets for the signal. From there, a subscriber drop provides the connection from the system to the subscriber's building.

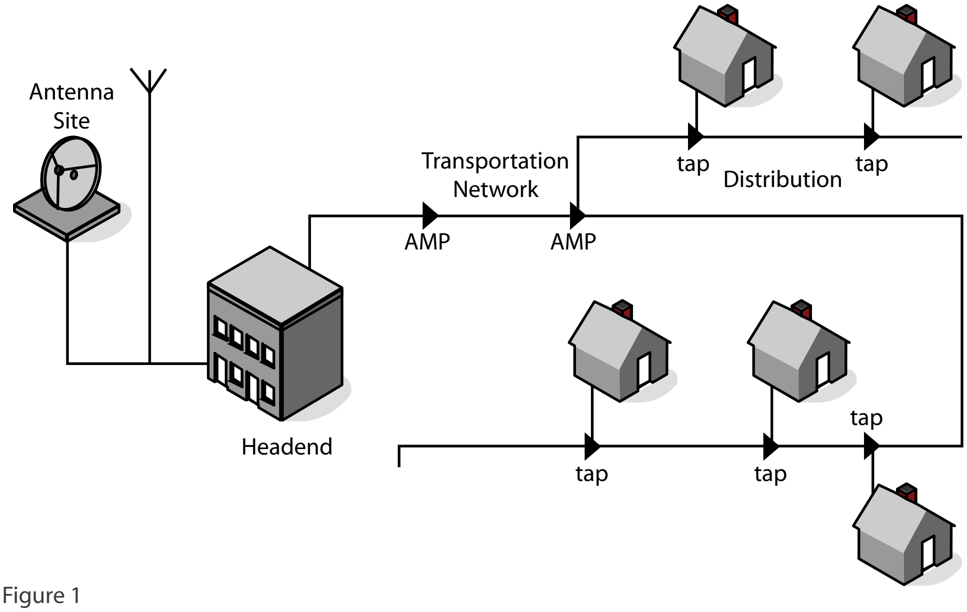


Figure 1

DOCSIS – Data Over Cable Service Interface Specifications

The specification for cable Internet and modems is DOCSIS, which you can see below. Each brought new enhancements for cable Internet. Currently, DOCSIS 2.0 is being used.

DOCSIS 1.0 – Developed in 1997.
DOCSIS 1.1 – Developed in 1999.
DOCSIS 2.0 – Developed in 2002, implemented QoS and VoIP.
DOCSIS 3.0 – Currently in development but will include channel bonding. This is tying together multiple channels to make a larger pipe.

Downstream uses 50 Mhz – 860 Mhz in the RF spectrum and can be divided up in 6 MHz chunks.
Upstream uses 5 Mhz – 42 MHz in the RF spectrum.

Cable Modem Boot Process

After power-up, the cable modem scans the frequencies for the downstream signal. Once it finds the downstream, it negotiates the upstream frequency. Once these are established, the layer 1 and 2 OSI path is completed. Now the modem asks for an IP through DHCP and is assigned one by the headend. Once the IP is assigned, then TFTP (trivial FTP) takes place and the DOCSIS config is downloaded to the modem. This provides downstream and upstream frequencies, TV sections, VoIP and QoS settings. Now the cable modem will register its MAC address with the service and completes the layer 3 section.

Describe xDSL Technologies

The DSL technologies have two transmission modes, synchronous (same upstream and downstream speeds) and asynchronous (faster downstream speed and slower upstream speed). DSL is transmitted over the same copper wires your voice phone operates on, as voice traffic only uses up a small portion of the frequency on the line. DSL uses the unused portion above the voice area, allowing both phone calls and Internet service. A filter is used to keep the data signals from interfering with the voice calls. The filter can be installed either where the phone line enters the building, effectively filtering all phones, or by installing a filter on each phone.

Due to running DSL over the same copper wires, there is a distance limitation. A DSLAM (DSL Access Multiplexer) is used to extend the distance from the central office (CO) to provide service to more customers.

DSL Frequency Ranges

The phone system uses 300 Hz to 3 kHz for voice and DSL uses the unused portion from 3 kHz to 1.1 MHz. This allows broadband Internet over existing phone lines.

DSL Variants

Variant	Downstream	Upstream	Max Distance
ADSL (a)	8 Mbps	1 Mbps	18,000 ft
G.SHDSL (s)	2.3 Mbps	2.3 Mbps	28,000 ft
IDSL (s)	144 kbps	144 kbps	18,000 ft
SDSL (s)	768 kbps	768 kbps	22,000 ft
VDSL (a/s)	52 Mbps	13 Mbps	4,500 ft

a – asynchronous; s – synchronous; G.SHDSL is an international standard maximum distance is measured from the CO to the subscriber's premises.

DSL Limitations

Apart from the distance limitations above, there are other factors that would preclude a customer from getting DSL server. If there is an older two wire system in the house, the wire can act as an antenna and pick up AM broadcast signals, causing interference with the DSL signal. This type of wiring can also cause cross-talk, the bleeding of one signal onto the other wire, degrading the signal. If the phone wires have been installed for a long time, there could be corrosion on the wires which would cause an impedance mismatch causing the signal to degrade.

Connection Methods

ADSL is the most popular and widely used type of DSL. It uses the entire frequency range on the phone line and requires the use of phone filters. A filter can be installed at each phone or device not using DSL, or you can install the filter at the phone box on the side of the building. Once this is done, all phones will be filtered inside the building and a separate line can be run just for the DSL modem.

RFC 1483 Bridged – This type of connection passes the connection directly to the PC. The PC will initiate a DHCP request and get an IP from the head end. This is not a secure connection as any device attached could get an IP without requiring authentication.

PPPoE – This is the most typical method of connecting to DSL. The PPP header is spliced into an Ethernet frame which adds the PPP features to the DSL connection. The only feature that is used is the authentication portion. A software install is needed on the PC to use the PPPoE authentication which is why it's easier to use a router. Cisco routers allow you to setup PPPoE connections on their routers.

PPPoA – This method has you connect the router directly to the ATM router. It still uses the PPP authentication but provides VPI/VCI information as well. The VPI/VCI information is like DLCI for frame relay or a MAC address on a network card.

Configuring PPPoE

To use DSL as your connection, the router has to have a dialer interface configured along with PPP settings. Below are the settings that are needed.

PPPoE on Ethernet Interfaces – On a router with two interfaces, PPPoE functionality is configured on the provider facing interface.

Configure a Dialer Interface

```
interface Dialer1
 ip address negotiated
 ip mtu 1492
 ip nat outside
 encapsulation ppp
 dialer pool 1
 ppp authentication pap callin
 ppp pap sent-username mydslconn@isp.com password 0 123456
```

Interface dialer 1 is a virtual interface that will handle the PPPoE authentication and actually get the IP address from the ISP by use of the **ip address negotiated** line. Since this is PPPoE, the connection has to be authenticated before an address can be handed out. By setting the MTU to 1492, this will allow you to use the full MTU of 1500, since PPPoE has an 8k header. IP nat outside is used to translate the private address to the public address when someone goes to the Internet. Encapsulation ppp tells the interface it is using the PPP protocol for this connection. Dialer pool 1 will be used to virtually connect this interface with a physical interface. PPP authentication pap callin tells the interface that we are using PAP (password authentication protocol) to send the username and password by connecting to the DSL provider. PPP pap sent-username and password is the line where you would insert the username and password for the DSL connection.

Configure an Ethernet Interface

```
interface FastEthernet0
 no ip address
 duplex auto
 speed auto
 pppoe enable
 pppoe-client dial-pool-number 1
```

There are only two commands you have to apply to the Ethernet Interface: pppoe enable and pppoe-client dial-pool-number 1. The first command enables PPPoE on the interface and the second ties the interface to the dialer interface. An IP address will not be assigned to the interface since the dialer interface will get the address from the provider.

Configure Port Address Translation

This is set by using the command ip nat outside on the WAN interface and ip nat inside on the LAN interface. Here is an example:

```
interface Dialer1
 ip address negotiated
 ip mtu 1492
 ip nat outside
 encapsulation ppp
 dialer pool 1
 ppp authentication pap callin
 ppp pap sent-username mydslconn@isp.com password 0 123456
!
interface Vlan1
 ip address 10.10.10.254 255.255.255.0
 ip nat inside
```

Since the statements are applied to the interfaces, we need to tell the interfaces what to NAT. This is done by setting up an access list and globally assigning NAT to the access list.

```
ip access-list extended NAT_ADDRESSES
 permit ip 10.10.10.0 0.0.0.255 any

ip nat inside source list NAT_ADDRESSES interface Dialer1 overload
```

The overload command allows many internal users to get to the Internet. If the overload command is not applied, then only one device on the LAN will be allowed to the Internet.

Configure DHCP for LAN Users

You can setup the DSL router as a DHCP server for the LAN users. You will need to exclude the Ethernet interface of the router from the range by using:

```
ip dhcp excluded-address 10.10.10.254
```

The pool will be setup using the following commands:

```
ip dhcp pool PCLAN
 import all
 network 10.10.10.0 255.255.255.0
 default-router 10.10.10.254
```

Configure Static Default Route on the Router

In order to get to the Internet, a default route needs to be added to the router. By using the following command this can be obtained. It is always best to assign it to an Interface in case the IP address changes. This will prevent, or limit, the amount of reconfiguration and down time if changing ISPs.

```
ip route 0.0.0.0 0.0.0.0 Dialer1
```

Configuring PPPoA

PPPoA is Point-to-Point Protocol over ATM and will be configured on the ATM interface of the router.

VCMultiplexed PPP over AAL5 Known as VC-MUX or AAL5MUX, this provides the capability to create a per-protocol virtual circuit to transport payloads for differing routed protocols.

LLC Encapsulated PPP over AAL5 This uses a single virtual circuit to transport all protocols.

Configuration Using AAL5MUX

```
 interface ethernet0/0
  ip address 10.10.10.254 255.255.255.0

 interface ATM0/0
  no ip address
  dsl operating-mode auto
  pvc 8/35
encapsulation aal5mux ppp dialer
  dialer pool-member 1
```

Configuration Using AAL5SNAP

```
interface ATM0/0
 no ip address
 dsl operating-mode auto
interface ATM0/0.1 multipoint
 class-int ppp-default
 pvc 8/35
```

```
vc-class atm ppp-default
 encapsulation aal5snap
 protocol ppp virtual-template 1
 ubr 256
```

Configuring the PPPoA DSL Dialer and Virtual-Template Interfaces

```
interface ATM0/0
 no ip address
 dsl operating-mode auto
 pvc 8/35
 pppoe-client dial-pool-number 1

interface Dialer0
 ip address negotiated
 ip mtu 1492
 encapsulation ppp
 dialer pool 1
```

Similar to the regular PPPoE configuration except you are using an ATM port

Virtual Template Configuration

```
interface virtual-template1
 encapsulation ppp
 ip address negotiated
 ip nat outside
 ppp authentication chap
 ppp chap hostname dslrouter@dslnetwork.com
 ppp chap password 0 12345
```

Virtual templates are logical interfaces, much like dialer interfaces.

Verify Basic Teleworker Configurations

Since cable Internet is similar to a regular WAN connection, you can troubleshoot it in a similar manner to troubleshooting a network issue.

With DSL, everything you can troubleshoot is based on the first two layers of the OSI model: physical and data link layer.

Isolating Physical Layer Issues

Layer 1 anatomy – There are two distinct functions which are performed at layer 1. These are some form of transmission convergence (TC) sublayer and a physical medium dependent (PDM) sublayer. This means the bits have to be placed in a particular order as per protocol between endpoints. This is known as framing. A simple translation is: the TC and PDM line up the bits and kick them out the interface.

ADSL Physical Connectivity

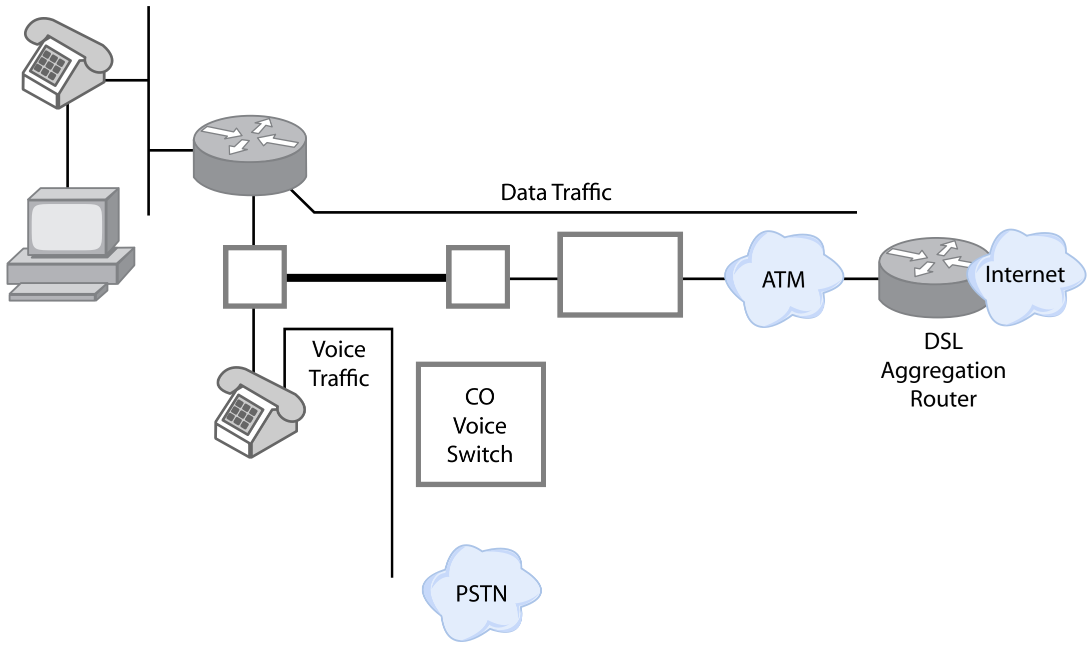


Figure 2

There are a number of individual segments that physical connectivity relies on for a DSL connection to function properly. As each device is encountered, as seen in figure 2 above, the PMD and TC sublayers perform their "line up the bits and kick them out the interface" function, even if each egress is a different media type. If there is a wiring fault between the subscriber and DSLAM, the result is the DSL modem not being able to negotiate with the DSLAM. This will result in a failure of the PPP connection and subsequently IP connectivity.

Troubleshooting Steps

An easy way to begin is by issuing the **sho ip int brief** command and make sure the interfaces show a status of up and protocol as up. If this is the case, then the interface is functioning and layers 1 and 2 can be ruled out as the problem. The status is layer 1 and the protocol is layer 2. If the interface shows down or is flapping, going down then up and repeating, then the issue is at layer 1. If layer 1 is down, then layer 2 will be down; this is due to layer 2 being dependent on layer 1 being up.

If, while looking at the interface, you see the interface as "administratively down," go into that interface and issue the "no shutdown" command. This will enable the interface and should bring it up. If not, then employ other network troubleshooting steps to isolate the problem.

To look at each interface, issue the command **sho int atm 0** or whichever interface you wish to look at. You can glean information from the statistics on each port. You will see various counts, such as packets transmitted and received, runts, giants and some others, that would allow you to assess the port.

If the ATM port is not functioning properly, check the configuration and make sure you have everything needed. Remember, with a PPPoA connection, as opposed to PPPoE, you have to have a PVC defined in the configuration.

Some things to look for would be the LEDs on the devices. As the old saying goes, "if it's green, it's good." As a device is powered on, the LEDs for the ports as well as other functions of the device will change color. During the initialization phase, the LED will be either red or amber. Once the port is up, the LED should change to green. If you are uncertain as to what color the LED should be, consult the devices manual.

In some installations cables can be an issue. Make sure the cables and wires connecting the devices are untangled and not stretched to their limit. Also, check the connectors on the cables. A loose connector will cause connectivity issues. Either cut off the end and crimp a new one on or replace the cable completely.

If the cables look to be in good shape and not contributing to the problem, then debug commands on the router can help determine a connectivity issue. If you are uncertain which debug commands to use, then issue the "debug ?" command to get a listing. Since you are dealing with DSL, you would use the **debug ppp negotiation** and **debug ppp authentication** commands. This will show if the device is negotiating correctly with the head end and whether the user name and password is causing a problem.

Listed in Table 1 is the bottom up troubleshooting information starting with layer 1.

Layer	**Components**	**Dependency**
Network layer	Routing and routed protocols	Layers 1 and 2 active
Data Link layer	Media-specific addressing and framing information	Layer 1 active
Physical layer	PMD and TC sublayers for transmission and bit order	Framing and line code

Table 1

When using an ATM connection, issue the **debug atm events** and **debug atm packets** commands. The output of the debug atm events shows the current VPI and VCI on which traffic is being received. The debug atm packets command shows the current state of ATM traffic hitting the interface and what the encapsulation type is. Table 2 shows what information you get with each of the debug commands.

Command	**Purpose**
debug atm events	Verifies ATM VPI/VCI configuration
debug atm packets	Verifies ATM encapsulation and circuit protocol
debug ppp negotiation	Verifies PPP LCP option negotiation
debug ppp authentication	Verifies PPP authentication

Table 2

Implement Frame-Mode MPLS

Multiprotocol Label Switching (MPLS) is a WAN technology primarily used by service providers. Now it is being implemented as a way for businesses to connect branch offices more efficiently. Table 3 lists WAN topologies and their pros and cons. Table 4 lists switching mechanisms.

Topology	**Pros**	**Cons**
Hub-and-spoke	Low-cost connectivity	Single point of failure at hub
Partial mesh	Some redundancy with moderate cost balance	Significant service impact due to outages at key sites
Full mesh	Fully redundant	High cost
Redundant hub-and-spoke	More redundant than hub-and spoke	Significant service impact due to outages at key sites

Table 3

Switching Mechanism	**Pros**	**Cons**
Process switching	Recursive routing lookup Updates at all times	Slow and every packet gets checked
Fast Switching (a.k.a. cache-driven)	Interrupt code driven, faster than process switching	First packet process switched. Difficult to load balance
CEF switching (a.k.a. topology-driven)	Full load balancing capable	High memory and CPU utilization

Table 4

MPLS Components

There are two major components to MPLS: **control plane** which maintains routing and label information exchange between adjacent devices and **data plane** which forwards traffic based on destination addresses or labels.

The control plane will include routing protocols such as EIGRP, OSPF, IS-IS, BGP and such. The label based routing protocols are **tag distribution protocol (TDP)** and **label distribution protocol (LDP)**. TDP is Cisco proprietary, created prior to any standard for MPLS, and LDP is the industry standard. Cisco dropped TDP altogether but can still be implemented if using strictly Cisco devices.

MPLS provides an MPLS traffic engineering (MPLS TE) mechanism that allows bandwidth reservation with **resource reservation protocol (RSVP)**. RSVP allocates bandwidth on demand and is typically used for voice traffic or other highly critical/time-sensitive traffic definition.

The **label forwarding information base (LFIB)** is created to store label information for use by the forwarding engine and is obtained from the routing protocol or LDP. This provided by the data plane and this is its sole existence.

MPLS Labels

The labels function to separate forwarding operations from layer 3 destinations in the packet headers. Labels become a highly efficient source of forwarding information by associating a label with a forwarding equivalence class (FEC). An FEC is a group of IP packets that are forwarded over the same path, in the same manner and the same forwarding treatment per-hop. They may correspond to a destination IP network or to any traffic class the LSR (label switching router) deems significant.

The edge LSRs add labels to the packets. The provider edge router is the edge LSR, but this may not be the case as the provider's architecture determines the location of the edge LSRs.

In frame mode MPLS, the label is inserted between the layer 2 and layer 3 headers and is stored in their various FECs without the need to examine the layer 3 header. Figure 3, below, shows the various connections and devices.

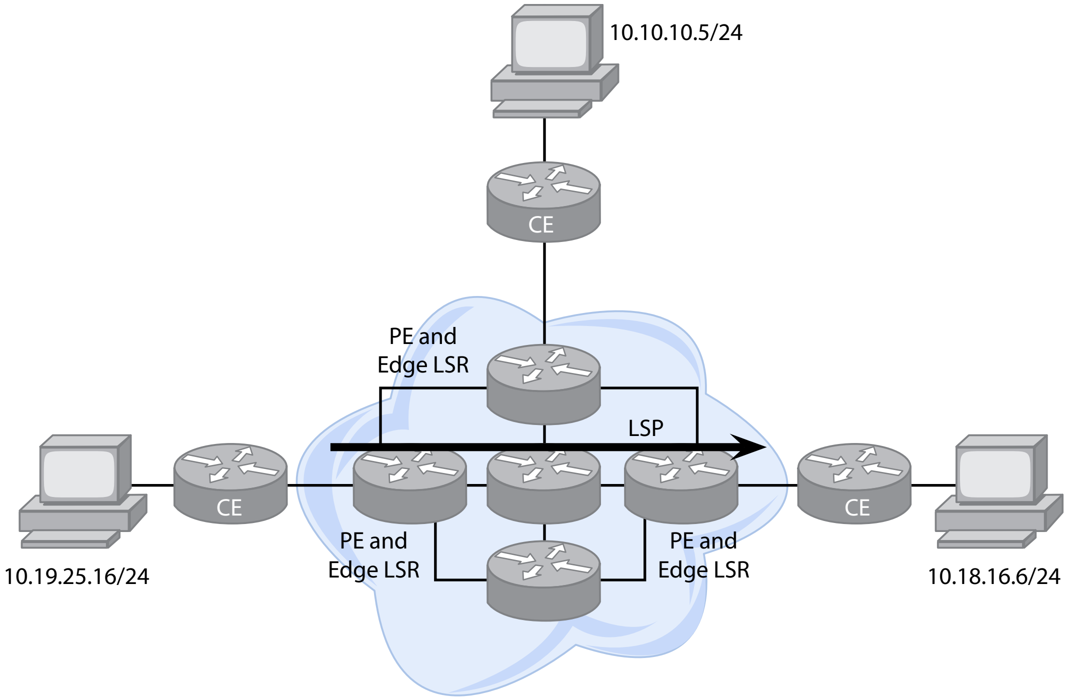


Figure 3

20 Bits	3 Bits	1 Bit	8 Bits
Label	EXP CoS	S	TTL

The label shown above is a 32 bit structure which includes the following fields:

- Label – 20 bits
- Experimental CoS (Class of Service) – 3 bits
- Bottom of Stack Indicator – 1 bit
- Time To Live – 8 bits

The label field itself can be any number from 0 to 1,048,575, but 0 to 15 are reserved for future use, so labels will start with 16. The labels can be stacked in the header as seen below.

Frame Header	Label 3 S=0	Label 2 S=0	Label 1 S=1	Layer 3 protocol header	Payload

Frame Mode MPLS

Frame mode MPLS denotes the use of MPLS with Ethernet-encapsulated or other frame-based-encapsulated interfaces. It does not include ATM-encapsulated interfaces. ATM uses cell mode MPLS and has a unique set of requirements.

When a PE router receives a packet, it makes a decision like any other router. It imposes the label and encapsulates the packet in the proper layer 2 framing structure if the outbound interface is MPLS-enabled.

Table 5 shows the two planes that are used in MPLS and what function they perform.

Plane	**Purpose**
Control plane	Label and routing information exchange
Data plane	Forward packets based on labels

Table 5

Table 6 shows the forwarding methods and how they are created.

Table	Built By	Contains	Purpose
FIB	IGP routing processes	Known destination prefixes, outbound interfaces, and next-hop addresses	Maps destination networks to next-hop address and outbound interface
LIB	LDP or other label distribution method	Local labels, FEC, LDP information	Associate local labels with FECs
LFIB	IGP and LDP information	Label-in, FEC, out-interface, label-out	Database used to forward labeled packets to next-hop address
Adjacency table	Forming of neighbor relationship	Out-interface and encapsulation along with neighbor ARP information	Maintain needed layer 2 information as well as LDP exchange capabilities

Table 6

Configuring Frame Mode MPLS

To enable MPLS, three steps need to be performed on the router, which are listed below:

- **Configure CEF** – This must be enabled prior to enabling MPLS.
- **Configure MPLS on a Frame Mode Interface** – The MPLS backbone interfaces should be MPLS-enabled and will generally be the WAN port on the router.
- **Configure MTU size as needed** – To keep frames from going over the MTU size on the interface, the MTU should be adjusted in MPLS-enabled interfaces.

Configuring CEF

CEF is extremely fast and efficient and is an advanced layer 3 switching technology which optimizes the performance and stability of networks with large, dynamic traffic patterns. It uses the FIB, which is a mirror copy of the routing table, instead of a route cache to eliminate fast/process switching and cache maintenance of packets.

CEF is enabled as a global command on the router as shown below.

```
Router(config)#ip cef
```

This will enable the central mode and is one instance of CEF. By using the following command, distributed mode can be enabled and should be used on high-end routers.

```
Router(config)#ip cef distributed
```

To enable CEF on a particular interface, the following commands are issued:

```
Router(config)#int e0/0

Router (config-if)#ip route-cache cef
```

Some options available for CEF configuration include the following:

- **CEF load balancing** – Can be configured for per-destination or per-packet load balancing.
- **CEF network accounting** – Allows collecting of traffic statistics such as packets and bytes switched to a particular prefix.
- **CEF distributed tunnel switching** – Enabled automatically with CEF, this option allows the switching of tunnels such as GRE tunnels. This option is not configurable.

Issue the **show ip cef** command to monitor and view CEF statistics. You can also issue the **show ip cef detail** command to display more detailed information about CEF. Command parameters are shown in Table 7 below.

Parameter	**Description**
unresolved	Displays unresolved FIB entries
summary	Displays a FIB summary
adjacency	Displays FIB entries known via a particular interface and next-hop address
A.B.C.D	Displays a FIB entry for a specific destination network
A.B.C.D A.B.C.D	Displays a FIB entry for a specific destination network and mask
longer-prefixes	Displays a FIB entry for all specified destinations
detail	Displays detailed FIB information
type number	Displays interface-specific FIB entries

Table 7

Commands such as **clear adjacency**, **clear ip cef inconsistency** and **clear cef interface** can be used if the network becomes unstable or a single router is unable to properly maintain the juggling act imposed upon it. Real-time monitoring of events on a particular router can be obtained by using **debug ip cef** and **debug ip cef events**.

Configuring MPLS on a Frame Mode Interface

To enable MPLS on a router, the **mpls ip** command is issued as a global command. Once done, the same command is issued for each interface on which MPLS will run. After enabling MPLS on the interface, the label distribution protocols must also be enabled by using **mpls label protocol**. Tag Distribution Protocol (TDP) is not typically used since it is Cisco proprietary. The Label Information Base (LIB) is created by the Label Distribution Protocol (LDP). Table 8 shows the parameters available with the **mpls label protocol** command.

Parameter	Description
both	Use LDP or TDP (adapt to peer on multi-access interface)
ldp	Use LDP
tdp	Use TDP

Table 8

A sample is shown below.

```
ip cef
!
interface GigabitEthernet0/1
ip address 10.10.1.1 255.255.255.0
duplex full
speed 1000
mpls label protocol ldp
mpls ip
```

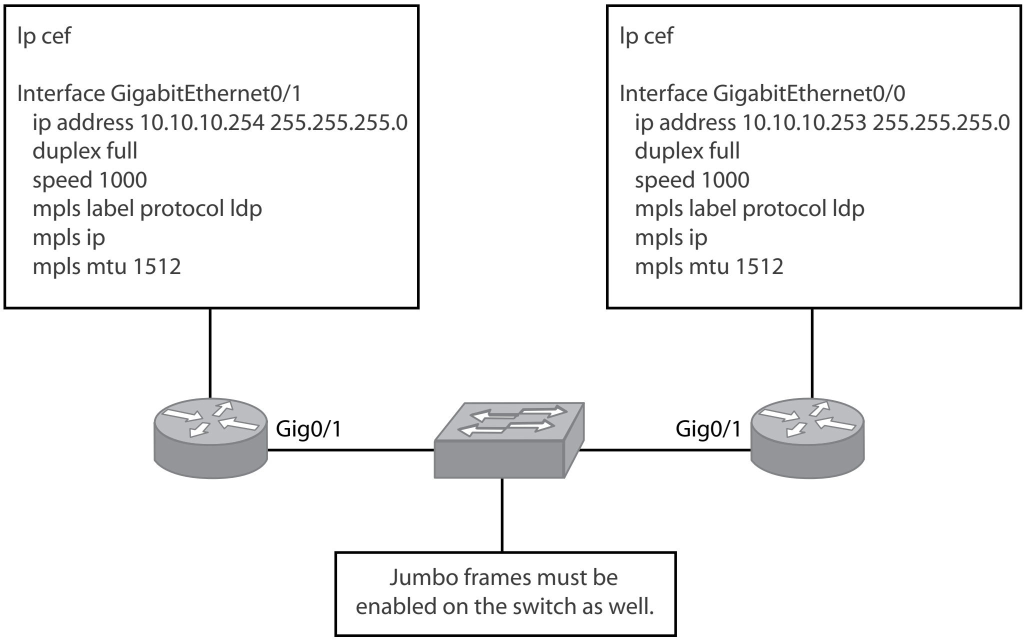
Configuring MTU Size

The MTU size is generally adjusted on an Ethernet interface since the addition of MPLS labels will increase the size of the packet. This will eliminate giants, baby giants or jumbo frame errors on the interfaces. WAN interfaces usually have larger MTUs by default or will adjust dynamically.

```
router(config-if)#mpls mtu 1512
```

The above command is MPLS-specific and will not affect other traffic. The valid range of MTU sizes is 64 to 65,535.

Figure 4 shows MPLS MTU configuration requirements.



```
Ip cef

Interface GigabitEthernet0/1
  ip address 10.10.10.254 255.255.255.0
  duplex full
  speed 1000
  mpls label protocol ldp
  mpls ip
  mpls mtu 1512
```

```
Ip cef

Interface GigabitEthernet0/0
  ip address 10.10.10.253 255.255.255.0
  duplex full
  speed 1000
  mpls label protocol ldp
  mpls ip
  mpls mtu 1512
```

Jumbo frames must be enabled on the switch as well.

Figure 4

To ensure LDP adjacencies have been established, use the **show mpls ldp neighbor** command, a sample of which can be seen below.

```
router#sh mpls ldp neighbor
    Peer LDP Ident: 192.168.1.1:0; Local LDP Ident 3.3.3.3:0
        TCP connection: 192.168.1.1.17080 - 3.3.3.3.646
        State: Oper; Msgs sent/rcvd: 17/18; Downstream
        Up time: 00:07:01
        LDP discovery sources:
                GigabitEthernet0/1, Src IP addr: 10.10.10.253
        Addresses bound to peer LDP Ident:
                172.16.0.4          192.168.1.1          10.10.10.253
router#
```

To show the exchange of label information regarding each network prefix in the routing table, issue the **debug mpls ldp bindings** command.

Table 9 shows the MPLS configuration steps.

Configure	Command	Configuration Mode	Parameters
CEF	**ip cef**	Global	**distributed**
MPLS	**mpls ip**	Global	**default-route** **propagate-ttl** **ttl-expiration**
MPLS	**mpls ip**	Interface	**encapsulate**
LDP or TDP	**mpls label protocol**	Interface	**both, tdp, ldp**
MTU	**mpls mtu**	Interface	**64 – 65,535**

Table 9

MPLS VPNs

MPLS VPNs take the best of both overlay and peer-to-peer VPNs. Through the use of a route distinguisher (RD) that is unique to a particular customer, each customer's information is kept securely, separate from every other customer's routing information. The use of the RD allows each customer to be given a logically separate PE router, though not necessarily physically separate.

Customer routing information is maintained by a specific routing protocol instance tied to its RD. A virtual routing and forwarding (VRF) table is the routing table which is assembled by this routing protocol instance. VRF provides isolation between customer routes.

Since most customers will be using RFC 1918 addressing, there is a need to keep individual customer routes separate and distinct. This is accomplished with the route distinguisher, which is a 64-bit identifier that is tacked onto the front of the IPv4 address. These are advertised between BGP peers on PE routers. This is known as Multiprotocol BGP.

To move customer routing information between the PE and CE routers, an IGP runs across the local loop. This is distributed into MPBGP where the prefixes are converted to VPNv4 addresses. RD values have no real specific meaning and are only meant to allow the routing architecture to deal with overlapping address space. The RD can be viewed as the VRF identifier in Cisco implementations.

A set of VPN identifiers can be attached to a route to indicate a membership to multiple VPNs. Route targets (RT) were introduced as an additional attribute which is attached to a VPNv4 BGP router to indicate VPN membership.

Table 10 shows MPLS VPN router roles.

Router	**Location**	**Purpose**	**Description**
C Router	C network, internal	Maintains C network routes and forwards traffic	A router internal to the customer-controlled network
CE router	C network, edge	Exchanges C network routes with a PE router	A customer-controlled router that interfaces and exchanges routing information with a PE router
P router	P network, internal	Maintains P network routes and forwards traffic	A router internal to the provider-controlled network, usually an LSR
PE router	P network, edge	Exchanges VPN routes with CE router	A provider-controlled router that interfaces and exchanges routing information with a CE router

Table 10

Table 11 shows MPLS VPN related protocols.

Protocol	**Where**	**Description**
Customer IGP	C network and CE-PE router connection	The customer internal routing protocol used to maintain routing information throughout the enterprise
Provider IGP	P network	The provider internal routing protocol used to maintain routing information, usually BGP, IS-IS, and/or OSPF
MPBGP	PE-to-PE peering	Multiprotocol BGP maintaining peer connections between PE routers for the express purpose of propagating C network routing information

Table 11

Implement a Site-to-Site IPSec VPN

Describe the Components and Operations of IPSec VPNs and GRE Tunnels

IPSec VPNs have two modes, transport mode and tunnel mode. Transport mode is from an end client PC on a LAN which encrypts data across the LAN. Tunnel mode is used for site-to-site VPNs where the connection is secure and the data is encrypted across the Internet.

Table 12 shows the features of IPSec.

Data confidentiality	Making sure no one sees the data – encryption
Data integrity	What was received is what was sent – hashing
Data origin authentication	Ensuring the other side is who they say they are
Anti-replay	Keep duplicate packets out of the VPN – someone resending packets to get into the network

Table 12

IPSec Protocols

IPSec consists of three primary protocols which help implement the overall architecture. Table 13 lists the protocols. Note that AH does not provide data confidentiality.

Internet Key Exchange (IKE)	A framework for negotiation and exchange of security parameters and authentication keys
Encapsulating Security Payload (ESP)	A framework for the data confidentiality, data integrity, data origin authentication and optional anti-replay features
Authentication Header (AH)	A framework for the data integrity, data origin authentication and optional anti-replay features

Table 13

The following encryption methods are available to ESP:

- **Data Encryption Standard (DES)** – An older method of encrypting information which has enjoyed widespread use.
- **Triple Data Encryption Standard (3DES)** – A block cipher using DES three times.
- **Advanced Encryption Standard (AES)** – One of the most popular symmetric key algorithms used today.

Authentication header (AH) does not hide (encrypt) the data but ensures the data has not been modified during transit. AH, as well as ESP, uses Hash-based Message Authentication Code (HMAC) as the authentication and integrity check. Table 14 lists the two hash algorithms which can be used. Both MD5 and SHA-1 use a shared secret key for both the calculation and verification of the message authentication values.

Hash Algorithm	**Input**	**Output**	**Used by IPSec**
Message Digest 5 (MD5)	Variable	128 bits	128 bits
Secure Hash Algorithm (SHA-1)	Variable	160 bits	First 96 bits

Table 14

The endpoints of the IPSec VPN must be validated before IPSec can secure the data transfer. Peer authentication certifies the remote IPSec endpoint is who it says it is using one of five methods. Table 15 lists the five methods to authenticate an IPSec peer.

Username and Password	Predefined and preconfigured on each endpoint – not very safe - is used for long periods of time
One-time Password (OTP)	Used for one instance of a VPN connection using either a PIN or TAN
Biometrics	Physical human characteristics such as fingerprint, retina scan, etc., authenticating who is at the originating end
Preshared keys	A single key, like username/password, preconfigured at both end points and must be safeguarded
Digital certificates	Issued to a device from trusted third-party CA. Certificate is only good for the device it was issued to

Table 15

IKE Protocols

The means of exchanging IPSec parameters and keys dynamically is the function of the IKE protocol. To repel password attacks against IPSec sessions, IKE makes IPSec scalable by automating the key exchange/update process. It also helps to automatically establish security associations (SAs) between two IPSec endpoints. An SA is the agreement of IPSec parameters between two peers.

IKE uses other protocols to perform peer authentication and key generation which are listed below.

- **ISAKMP** – The Internet Security Association and Key Management Protocol defines how to establish, negotiate, modify and delete SAs. ISAKMP does not involve key exchange but does perform peer authentication.
- **Oakley** – The Oakley protocol uses the Diffie-Hellman algorithm to manage key exchanges across IPSec SAs.

IKE Phases

IKE uses two phases to create a secure communications channel between two endpoints which are primary and mandatory. But there is a third optional phase.

- **IKE phase 1** – A mandatory phase where a bidirectional SA is established between IPSec peers. The same key material is used by the data sent between the end devices. This phase may also perform peer authentication to validate the identity of the IPSec endpoints. Two IKE modes are available to establish the bidirectional SA. These are main mode and aggressive mode. Parameter negotiation, such as hash methods and transform sets, must agree or the connection cannot be established.
- **IKE phase 1.5** – This is an optional phase which provides an additional layer of authentication called Xauth, or Extended Authentication. Even though IPSec authentication in phase 1 authenticates the devices or endpoints, there is no means to authenticate the users behind the devices. Xauth forces the user to authenticate before use of the IPSec connection is granted by means of a username/password, CHAP, one-time password or secure key (S/KEY).
- **IKE phase 2** – Phase 2 is the other mandatory phase to establish an IPSec connection. Unidirectional SAs are implemented between the IPSec endpoints using the parameters agreed upon in Phase 1. Unidirectional SAs mean separate keying material is needed for each direction. IKE quick mode is used to establish each of the unidirectional SAs.

IKE Main Mode

This consists of six messages exchanged between the IPSec peers. Aggressive mode is not used if main mode is selected and quick mode always follows main mode. The six messages can be broken down into three pairs. Table 16 lists the three pairs.

IPSec parameters and security policy	One or more proposals are sent and the responder selects the appropriate one.
Diffie-Hellman public key exchange	Public keys are sent between the two IPSec endpoints.
ISAKMP session authentication	Each end is authenticated by the other.

Table 16

IKE Aggressive Mode

This is an abbreviated version of main mode and, if selected, main mode is not used. The six packets of main mode are condensed into three:

- All data, IPSec parameters, security policies and Diffie-Hellman public keys are sent by the initiator.
- Once the responder authenticates the packet, it sends the parameter proposal, key material and identification back.
- The initiator authenticates the packet.

IKE Quick Mode

Quick mode is used during IKE phase 2 and is protected by the IKE SA negotiated in Phase 1. Quick mode negotiates the SAs used for data encryption across the IPSec connection and manages the key exchange for those SAs.

IKE is a protocol that exchanges IPSec parameters and keys. There are other functions that are important to the setup and maintenance of the IPSec connection. Dead peer detection is accomplished by sending periodic keepalive timers between the IPSec peers. The timer should be fairly repetitive, such as every 10 seconds, to be effective. In this manner, the failure of the IPSec connection is recognized quickly by the loss of the hello packets. This, unfortunately, adds traffic that must be sent across the IPSec session.

NAT traversal solves one problem that NAT/PAT introduces. Since IPSec typically encrypts all data above Layer 3, the PAT translations, both IP addresses and ports shared by multiple inside devices to a single outside IP address, must be available in the transport layer headers. During phase 1, before quick mode, it is determined whether NAT is supported and whether NAT exists along the path of the proposed IPSec connection. Phase 2, quick mode, decides whether the IPSec peers will use NAT traversal and the negotiation occurs via the quick mode SA that is established.

By inserting a UDP header before the ESP header in the IPSec packet, NAT traversal is accomplished. The PAT translation process can successfully occur since the new transport layer header has unencrypted port information which can be stored in the PAT tables.

Encryption Algorithms

Encryption is a mathematical algorithm and key applied to data to make it unreadable to everyone except those who have the ability to decrypt it, which can only be done with the proper key. The complexity of the encryption algorithm and the size of the key used to encrypt the data determine the strength of the cipher text, the encrypted data.

Symmetric Encryption

Symmetric encryption is also called secret key cryptography and uses a single, secret key to both encrypt and decrypt the data. Anyone who manages to get the key can decrypt the data so it is important to keep the secret key a secret. Through the mid-1970s, this was the only type of encryption available and tends to be computationally easier to implement and is useful for large, bulk encryption requirements. Table 17 lists the three symmetric encryption algorithms used today.

DES	Using a 56-bit key, it has been broken in less than 24 hours using modern computers.
3DES	Applies three different 56-bit keys to create the cipher text. DES encrypt, DES decrypt, DES encrypt. It has not yet been broken.
AES	Considered the symmetric encryption choice today. Supports keys ranging from 128 bits to 256 bits and uses 64-bit increments and is the only symmetric encryption algorithm adopted by NSA.

Table 17

Asymmetric Encryption

Asymmetric encryption uses different keys to encrypt and decrypt data. The key used to encrypt the data cannot be used to decrypt it. A *public key* is used to encrypt the data and a *private key* is used to decrypt it. It is possible, and expected, to widely distribute the public key, and is only used to encrypt messages which will be decrypted with the associated private key. Digital signatures use the private key to sign a hash of the message and the public key decrypts and validates the signature. Similar to shared secret keys, private keys should be kept private.

The first algorithm that could be used for both signing and encrypting is RSA, which was named after its designers – Rivest, Shamir and Adleman. The key lengths for RSA start at 1024 and get longer typically by doubling the key length. Although not having been mathematically proven, it is thought to be impossible for full decryption of an RSA key due to the difficulty in factoring large prime integers. Asymmetric algorithms are not well suited for continuous, bulk encryption jobs due to being computationally expensive to implement.

The trick for symmetric encryption algorithms is keeping the secret key covert since the same key is used for encryption and decryption. This is not the case with asymmetric algorithms since there are separate keys for encryption and decryption. This makes asymmetric key exchange algorithms useful to safely deliver shared secret keys across an insecure network.

For the exchange of shared secret keys in IPSec, Diffie-Hellman is the primary asymmetric key exchange algorithm. The exchange process occurs in parallel between two IPSec peers. The interception of a public key does not cause any security concerns for an asymmetrical encryption algorithm since the private keys are never exchanged.

Public Key Infrastructure (PKI)

PKI provides a hierarchical framework for managing the security attributes of entities who engage in secure communications across a network. All of the IPSec devices mentioned in this Exam Manual are such entities, as well as the people who use those devices. PKI consists of a number of elements which are also network entities and are listed in Table 18.

Peers	End hosts, the devices and people who securely communicate across a network.
Certification authority (CA)	A trusted entity or a trust point that grants and maintains digital certificates.
Digital certificate	Contains the signature of the issuing CA, a signed copy of the public encryption key, information to uniquely identify a peer and certificate validity data. X.509v3 is the current digital certificate version.
Registration authority (RA)	An optional entity that can handle enrollment requests for the CA.
Distribution mechanism	LDAP and HTTP are examples of a means to distribute certificate revocation lists (CRLs) across the network.

Table 18

Any network entity who wishes to participate in secure communications receives a digital certificate. This contains a public/private key pair and has their identity validated by a CA. The exchange of certificates occurs when peers need to establish a secure communications channel. Table 19 details the message exchange process.

Step	Action
1	An end host generates an RSA key pair and requests the public key of its CA.
2	The CA sends its public key to the end host.
3	The end host generates a certificate request. Depending on the network configuration, either the request is automatically sent to the CA or manual intervention is needed to approve the request. The certificate request is sent to either the CA or the optional RA. The CA or RA receives the certificate request.
4	Once approved, the CA signs the certificate request with its private key. The CA returns the completed certificate to the end host.
5	The end host saves the certificate to some nonvolatile memory, such as disk, USB smart card or NVRAM.
6	The end host uses the validated certificate to establish secure communications with other end hosts which have accomplished these steps.

Table 19

Creating a Site-to-Site IPSec VPN

The lifecycle of any IPSec VPN has five generic steps and is explained below.

Step 1: Specify Interesting Traffic

Traffic that must be protected by the IPSec VPN is considered interesting traffic. This "interesting" traffic is sent securely through the VPN to the remote location when an IPSec VPN tunnel exists. If ESP is employed, the traffic cannot be read by anyone in the middle, nor can it be modified without detection. The capability to validate and decrypt the data is handled by the predetermined VPN endpoint and the data cannot escape from the VPN tunnel and travel to some unintended destination.

Any packets that are not interesting do not enjoy the benefits of the IPSec VPN. They may travel to any destination, including the remote destination where the VPN tunnel terminates, and are not encrypted or protected in any way.

In order to select which traffic is "interesting", extended access control lists are used. The ACL determines which traffic is permitted through the tunnel and applies the appropriate security policy. If the tunnel does not yet exist, the first packet of interesting traffic triggers the events needed to create the tunnel. The five steps of the IPSec VPN lifecycle assume the tunnel does not yet exist and must be built.

Step 2: IKE Phase 1

Once the first packet deemed interesting arrives, the process of creating the IPSec VPN tunnel begins. The second step in creating the tunnel is IKE phase 1. The basic purpose of main mode or aggressive mode is identical. However, the number of messages exchanged is greatly reduced in aggressive mode.

The first two exchanges in main mode negotiate the security parameters used to establish the IKE tunnel in the form of transform sets. The second pair exchanges the Diffie-Hellman public keys needed to create the secure IKE tunnel. This tunnel is later used to exchange the keys for the IPSec SAs. The final pair of packets performs peer authentication by using a hash function to confirm identity and ensure no rogue devices are permitted.

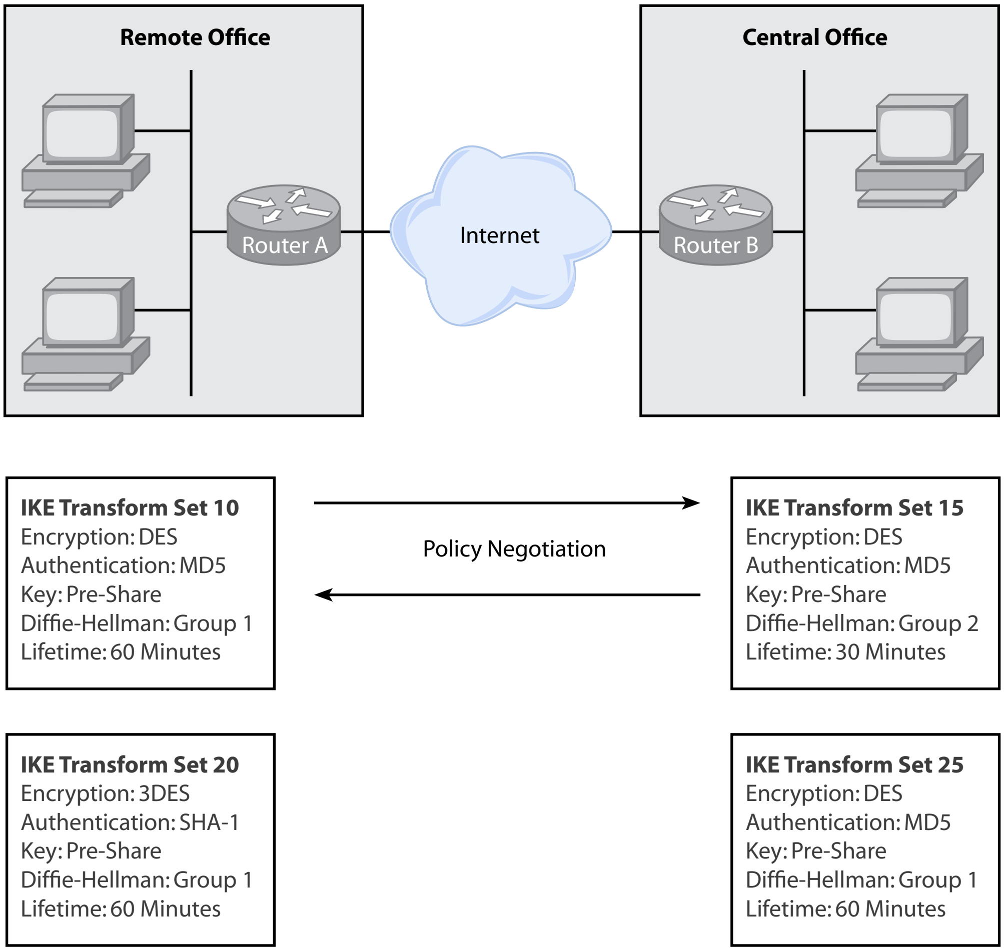
Aggressive mode reduces the IKE phase 1 exchange to three packets. The first packet is from the initiator to the receiver, which sends the security policy proposals, the Diffie-Hellman public key, a nonce which is signed and returned for identity validation and a means to perform authentication. The second packet is from the receiver back to the initiator and contains the accepted security policy proposal, its Diffie-Hellman public key and the signed nonce for authentication. The final packet is a confirmation from the initiator to the receiver.

IKE Transform Sets

Numerous individual parameters must be coordinated in IKE. Different combinations of security parameters are grouped into transform sets to avoid negotiating each one individually. These are setup on each endpoint. If both endpoints have a common policy then the setup of the IPSec VPN tunnel can continue. If there are no common parameter sets then the VPN process fails.

During IKE phase 1, these five parameters must be coordinated:

- IKE encryption algorithm (DES, 3DES or AES)
- IKE authentication algorithms (MD5 or SHA-1)
- IKE key (preshare, RSA signatures or nonces)
- Diffie-Hellman version (1,2 or 5)
- IKE tunnel lifetime (time and/or byte count)



IKE Transform Set 10
Encryption: DES
Authentication: MD5
Key: Pre-Share
Diffie-Hellman: Group 1
Lifetime: 60 Minutes

IKE Transform Set 15
Encryption: DES
Authentication: MD5
Key: Pre-Share
Diffie-Hellman: Group 2
Lifetime: 30 Minutes

IKE Transform Set 20
Encryption: 3DES
Authentication: SHA-1
Key: Pre-Share
Diffie-Hellman: Group 1
Lifetime: 60 Minutes

IKE Transform Set 25
Encryption: DES
Authentication: MD5
Key: Pre-Share
Diffie-Hellman: Group 1
Lifetime: 60 Minutes

Figure 5

Figure 5 shows how the two IPSec endpoints use IKE transform sets to coordinate the IKE tunnel. The contents of IKE police 10 on router A match those in IKE policy 25 on router B. Router B lets router A know it accepts policy 10 and the IKE SA is created. If router B did not have an exact parameter match in any of the transform sets then the IPSec tunnel would not be created and IKE would fail.

If there is only one remote location then only one transform set is needed. If there are multiple remote sites, then you can have a transform set for each remote site or use the same set for all.

Diffie-Hellman Key Exchange

The DH protocol is used to exchange the key material that will be used in phase 1 after the IKE policies have been agreed to. DH allows two parties to share a secret key over an insecure channel. Remember, it is important to keep the key secret.

Cisco VPN devices only support Diffie-Hellman groups 1, 2 and 5 which use 768-bit, 1024-bit and 1536-bit prime numbers respectively, even though there are a total of 7 groups. The larger the prime number, the longer it takes to generate the keys. However, the keys would be more secure. After the keys are exchanged and the shared secret is established, the SA for phase 1 is created. This SA is used to exchange key material for phase 2.

Peer Authentication

Authentication of the remote peer is the final step of IKE phase 1. This is important to keep rogue devices from connecting and establishing a tunnel. If this part fails, then the IPSec process stops and the tunnels are not created. There are three methods used for authentication:

- Preshared keys – manually entered into each peer.
- RSA signatures – use digital certificates to authenticate peers.
- RSA-encrypted nonces – a number that is used only once, similar to a one-time password.

Step 3: IKE Phase 2

This is where the IPSec tunnels are established. Phase 1 creates a very secure communications channel so that the tunnels can be created for data encryption and transport. The following functions are performed in IKE phase 2:

- Negotiation of IPSec security parameters via IPSec Transform sets
- Establishment of IPSec SAs (unidirectional IPSec tunnels)
- Periodic renegotiation of IPSec SAs to ensure security
- An additional Diffie-Hellman exchange (optional)

IKE phase 2 has a single mode called quick mode. If phase 1 is successful (main or aggressive mode), quick mode is used in phase 2. Quick mode encompasses the entire process that occurs in IKE phase 2.

First, each peer must negotiate the parameters that are used to create the tunnels. Similar to IKE phase 1, which uses IKE policies, transform sets are used during this process. Once the parameters are agreed upon, the SAs can be created, are unidirectional and two SAs are needed to have secure, bidirectional communication between two peers. Quick mode uses nonces to generate new key material for the shared secrets and to prevent replay attacks.

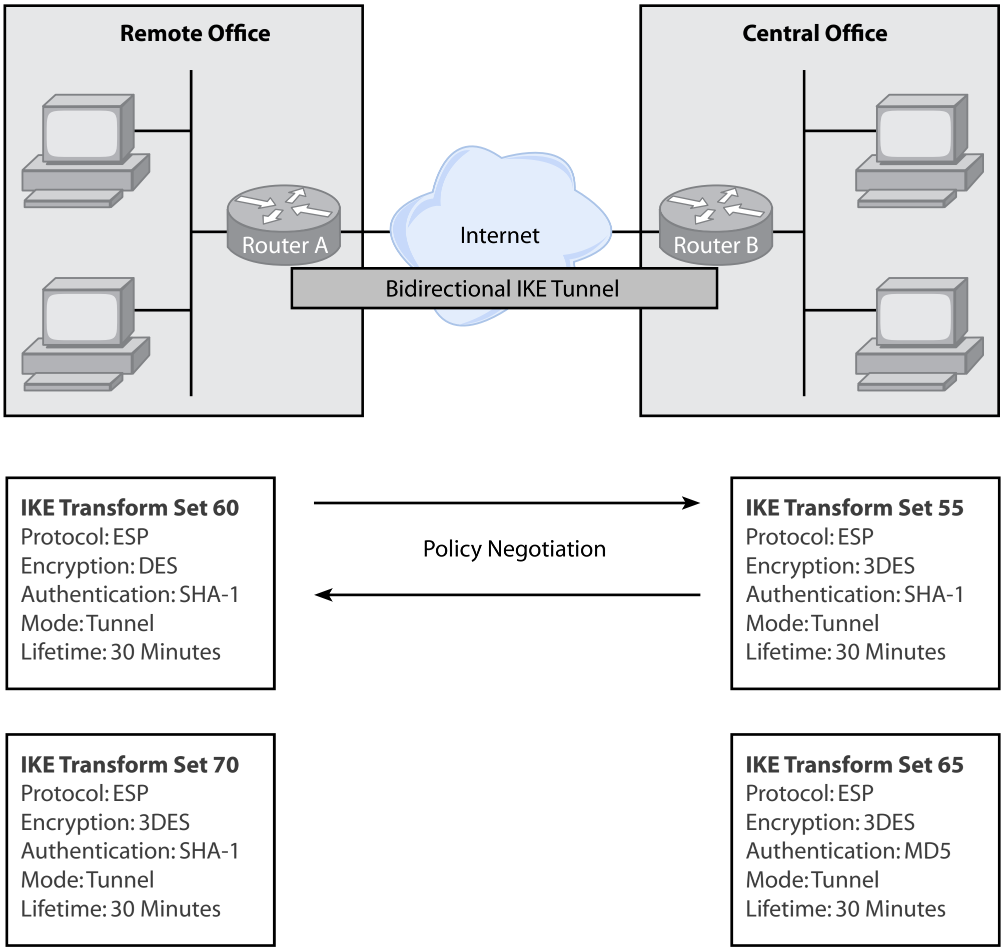
Quick mode monitors the expiration of SAs and establishes new ones when needed. An SA should never stay up indefinitely. This is to keep the encryption keys from being determined or compromised. A new SA is created near the end of the previous one's expiration so there is no loss of protected data flow.

IPSec Transform Sets

These are a group of attributes that are exchanged together which eliminates the need to coordinate and negotiate individual parameters. The attributes that are exchanged is the difference between an IKE policy and an IPSec transform set. Five parameters must be coordinated during quick mode between peers:

- IPSec protocol (ESP or AH)
- IPSec encryption type (DES, 3DES or AES)
- IPSec authentication (MD5 or SHA-1)
- IPSec mode (tunnel or transport)
- IPSec SA lifetime (seconds or kilobytes)

Figure 6 shows IPSec transform sets.



IKE Transform Set 60
Protocol: ESP
Encryption: DES
Authentication: SHA-1
Mode: Tunnel
Lifetime: 30 Minutes

IKE Transform Set 55
Protocol: ESP
Encryption: 3DES
Authentication: SHA-1
Mode: Tunnel
Lifetime: 30 Minutes

IKE Transform Set 70
Protocol: ESP
Encryption: 3DES
Authentication: SHA-1
Mode: Tunnel
Lifetime: 30 Minutes

IKE Transform Set 65
Protocol: ESP
Encryption: 3DES
Authentication: MD5
Mode: Tunnel
Lifetime: 30 Minutes

Figure 6

Just like in phase 1, the transform sets are sent from router A to router B. Router B compares the transform sets received to the ones it has. If there is a match, such as transform set 55 on router B and transform set 70 on router A, then router B responds to router A that it accepts set 70 and will use those parameters. If a match cannot be made then the IPSec SAs cannot be constructed and the IPSec process would fail.

Security Associations

An SA is a group of security parameters agreed upon between two IPSec peers. These parameters are exchanged during IKE phase 2 in the transform sets. Each IPSec SA is a one-way connection between two IPSec peers. Since effective network communications requires bidirectional traffic flow, a complete IPSec connection consists of two IPSec SAs – one incoming and one outgoing. Each SA is tracked and maintained separately but uses the same security parameters agreed upon in the IPSec transform sets.

A Security Parameter Index references each SA, travels with each IPSec packet and is used to reference and confirm the security parameters upon arrival at the far end. An SA Database (SAD) is used on each client to track each of the SAs it participates in. For any remote client, there will be two SAs and the SAD contains the following information about each IPSec connection:

- Destination IP address
- SPI number
- IPSec protocol (ESP or AH)

The Security Policy Database contains the security parameters that were agreed upon for each SA in the transform sets. This database contains:

- Encryption algorithm (DES, 3DES or AES)
- Authentication algorithm (MD5 or SHA-1)
- IPSec mode (tunnel or transport)
- Key lifetime (seconds or kilobytes)

SA Lifetime

The key lifetime is one of the security parameters that must be agreed upon in the IPSec transform set. The tunnel must not use the same key indefinitely due to the possibility of compromise. After a predetermined time or predetermined amount of data, the keys are forced to expire.

If data is flowing through the tunnel as the key expiration approaches, new keys are exchanged, new tunnels are built and the data stream is switched over to the new SAs. The lifetime values must not be too excessive so that the security of the tunnel is not exposed or compromised.

Step 4: Secure Data Transfer

Once the IPSec transform sets have been agreed upon by the endpoints, the SAD and SPD have been updated and traffic can flow through the tunnel. Remember, only the interesting traffic, as deemed by the ACLs, is permitted to use the tunnel. All other traffic continues to flow through the interface but not through the tunnel.

Step 5: IPSec Tunnel Termination

Only two events can cause an IPSec tunnel to be terminated. If the SA lifetime expires then the tunnel can be torn down. If secure transfer is still needed, then a new set of SAs is created before the old set is retired. An administrator can delete the tunnel manually or the tunnel can be torn down due to excessive time or kilobyte usage.

Regardless of the cause, all information about an SA is removed from both the SAD and SPD upon termination. The actual entries in the database are deleted but the security parameters about an SA may be copied to a new SPI as the secure data exchange continues.

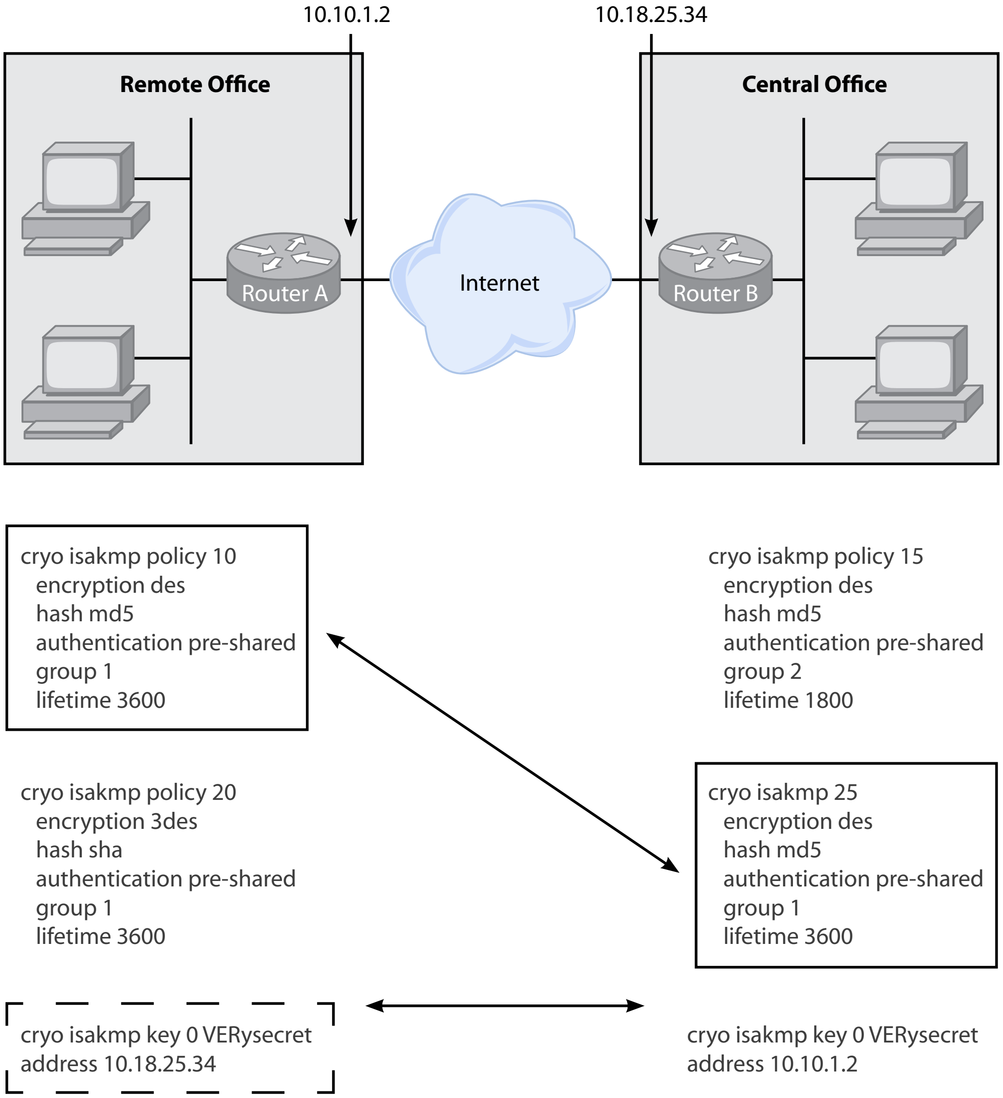
Site-to-Site IPSec Configuration Steps

There are six steps to configuring a site-to-site IPSec VPN. They are:

- Configure the ISAKMP policy (IKE phase 1)
- Configure the IPSec transform sets (IKE phase 2, tunnel termination)
- Configure the crypto ACL (interesting traffic, secure data transfer)
- Configure the crypto map (IKE phase 2)
- Apply the crypt map to the interface (IKE phase 2)
- Configure the interface ACL

Step 1: Configure the ISAKMP Policy

This step maps to IKE phase 1 which establishes a secure bidirectional tunnel used to exchange IPSec keys for the SAs. Figure 7 shows a sample configuration and how they relate to each other.



```
cryo isakmp policy 10
  encryption des
  hash md5
  authentication pre-shared
  group 1
  lifetime 3600
```

```
cryo isakmp policy 15
  encryption des
  hash md5
  authentication pre-shared
  group 2
  lifetime 1800
```

```
cryo isakmp policy 20
  encryption 3des
  hash sha
  authentication pre-shared
  group 1
  lifetime 3600
```

```
cryo isakmp 25
  encryption des
  hash md5
  authentication pre-shared
  group 1
  lifetime 3600
```

```
cryo isakmp key 0 VERysecret
address 10.18.25.34
```

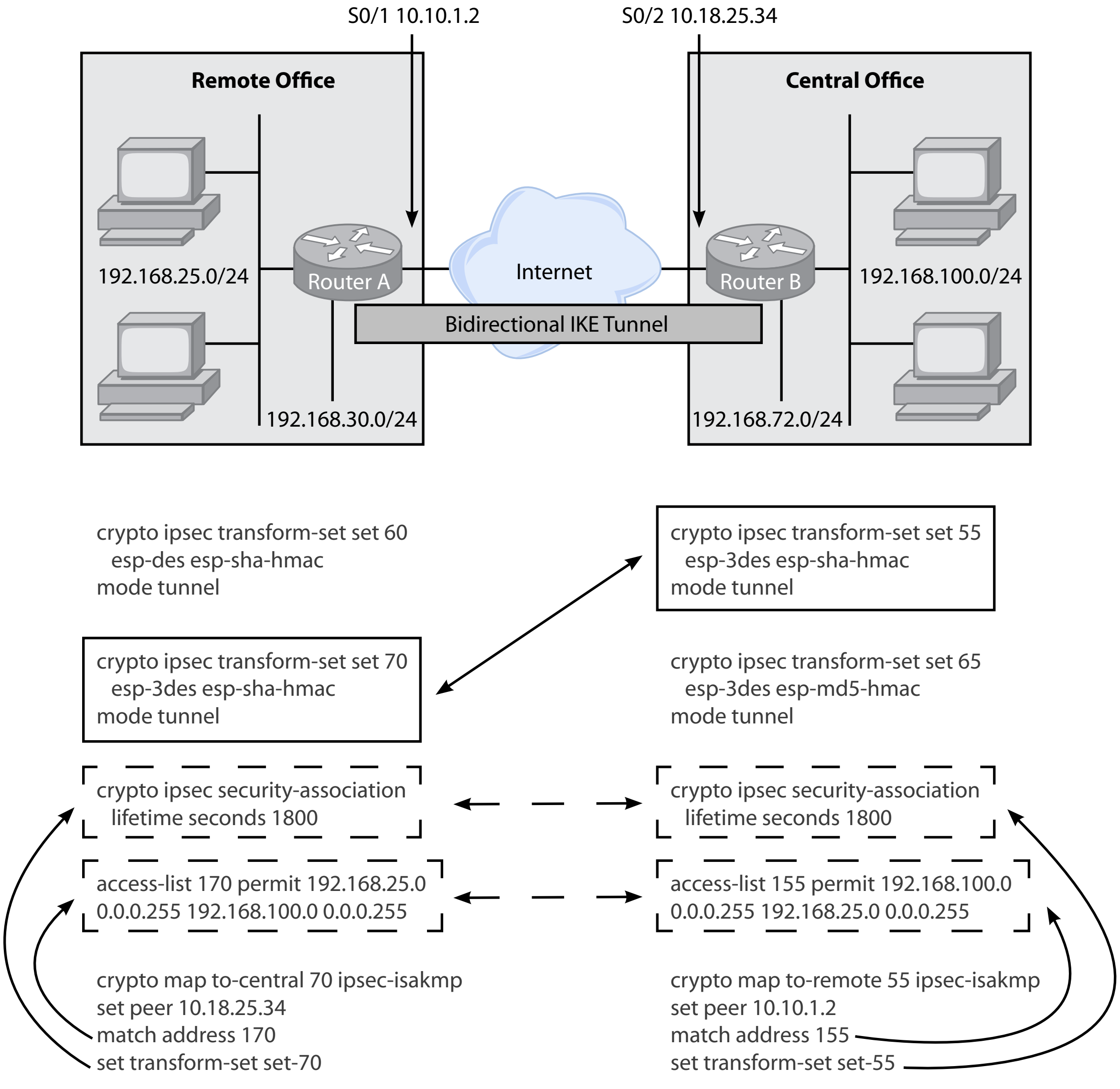
```
cryo isakmp key 0 VERysecret
address 10.10.1.2
```

Figure 7

IKE exchanges security parameters using IKE transform sets. There are two for each router shown in Figure 7. Each router also has two ISAKMP policies configured and since they are using pre-shared keys, the keys have to be defined. Since IKE policies are examined from the top down, the stronger IKE policies would have smaller numbers. This way, a weaker policy won't be agreed upon instead of a stronger policy.

Step 2: Configure the IPSec Transform Sets

This step actually covers three of the IPSec configuration steps listed above. The IPSec transform set, crypto ACL and crypto map are tightly woven together. This is shown in Figure 8.



```
crypto ipsec transform-set set 60
  esp-des esp-sha-hmac
mode tunnel

crypto ipsec transform-set set 70
  esp-3des esp-sha-hmac
mode tunnel

crypto ipsec security-association
  lifetime seconds 1800

access-list 170 permit 192.168.25.0
0.0.0.255 192.168.100.0 0.0.0.255

crypto map to-central 70 ipsec-isakmp
set peer 10.18.25.34
match address 170
set transform-set set-70
```

```
crypto ipsec transform-set set 55
  esp-3des esp-sha-hmac
mode tunnel

crypto ipsec transform-set set 65
  esp-3des esp-md5-hmac
mode tunnel

crypto ipsec security-association
  lifetime seconds 1800

access-list 155 permit 192.168.100.0
0.0.0.255 192.168.25.0 0.0.0.255

crypto map to-remote 55 ipsec-isakmp
set peer 10.10.1.2
match address 155
set transform-set set-55
```

Figure 8

Table 20 shows the IPSec transform sets.

Transform Type	**IOS Transform**	**Description**
AH Transform	ah-md5-hmac	AH with MD5 Authentication
	ah-sha-hmac	AH with SHA authentication
ESP Encryption Transform	esp-aes	ESP with 128-bit AES encryption
	esp-aes 192	ESP with 192-bit aeS encryption
	esp-aes 256	ESP with 256-bit AES encryption
	esp-des	ESP with 56-bit DES encryption
	esp-3des	ESP with 168-bit DES encryption
ESP Authentication Transform	esp-md5-hmac	ESP with MD5 authentication
	esp-sha-hmac	ESP with SHA authentication

Table 20

The **crypto ipsec transform-set** command is used to select an AH transform, an ESP encryption transform and/or an ESP authentication transform. Only one IOS transform from each transform type may be selected.

Step 3: Configure the Crypto ACL

To determine interesting traffic, an extended access list is used. In figure 8, the access list for the remote is number 170 while the access list for the central office is number 155. These lists define the source and destination addresses of traffic that will travel over the tunnel.

It is important that the two lists mirror each other. The source address in one list must the destination address in the other and vice versa. You cannot use a standard access list as it will not allow you to specify destination addresses.

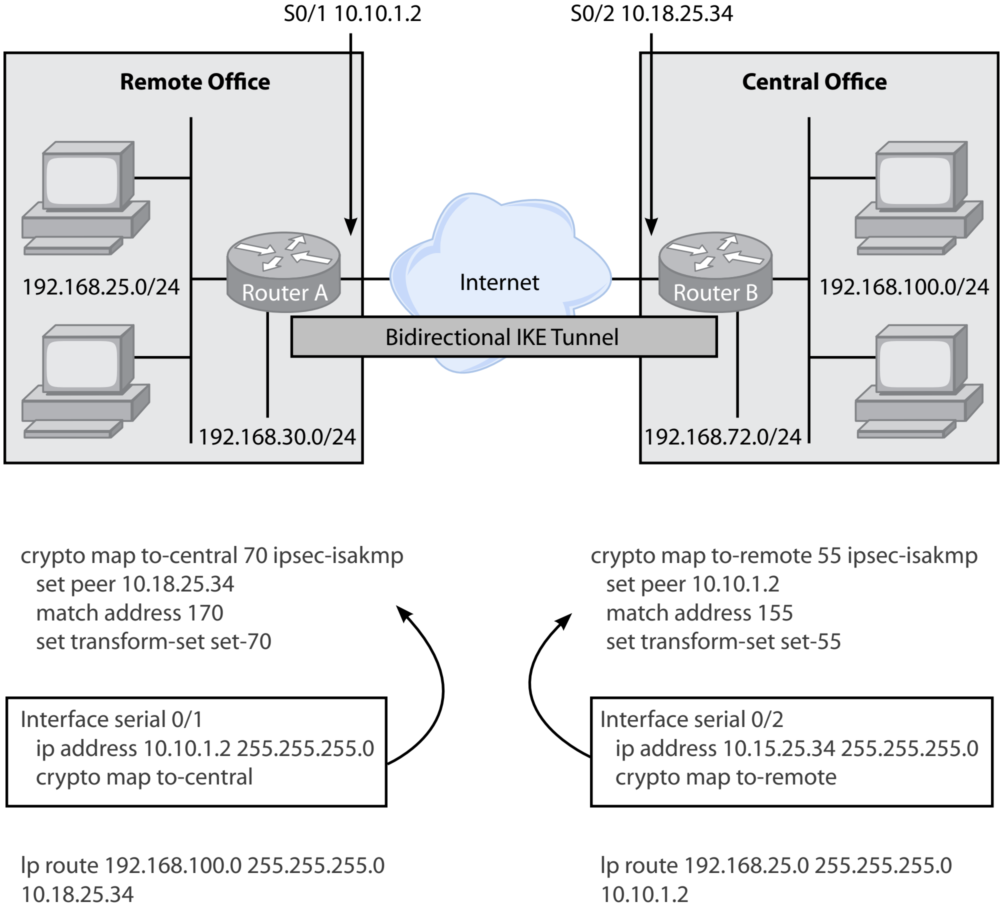
You can isolate the more advanced configuration to the main site by simply sending everything through the VPN tunnel to the main site from the remote. The main will only send traffic destined for the remote through the tunnel.

Step 4: Configure the Crypto Map

To tie the transform set and access it together, plus point them to a remote peer, you have to configure the crypto map. Each map can have multiple lines which are referenced numerically from the lowest to the highest. In Figure 8, numbers 70 and 55 in each of the crypto maps are the line numbers. For a router with a single interface but multiple remote VPN clients, a single crypto map must be used with a unique entry for each peer.

Step 5: Apply the Crypto Map to the Interface

After configuring the crypto map, it must be applied to an interface to be operational. The crypto map is a collection of the IP addresses of the remote peer, the interesting traffic that will flow through the IPSec tunnel and the IPSec security parameters that will be used to protect the data. Figure 9 shows the application of the crypto map to an interface.



```
crypto map to-central 70 ipsec-isakmp
  set peer 10.18.25.34
  match address 170
  set transform-set set-70

Interface serial 0/1
  ip address 10.10.1.2 255.255.255.0
  crypto map to-central

Ip route 192.168.100.0 255.255.255.0
10.18.25.34
```

```
crypto map to-remote 55 ipsec-isakmp
  set peer 10.10.1.2
  match address 155
  set transform-set set-55

Interface serial 0/2
  ip address 10.15.25.34 255.255.255.0
  crypto map to-remote

Ip route 192.168.25.0 255.255.255.0
10.10.1.2
```

Figure 9

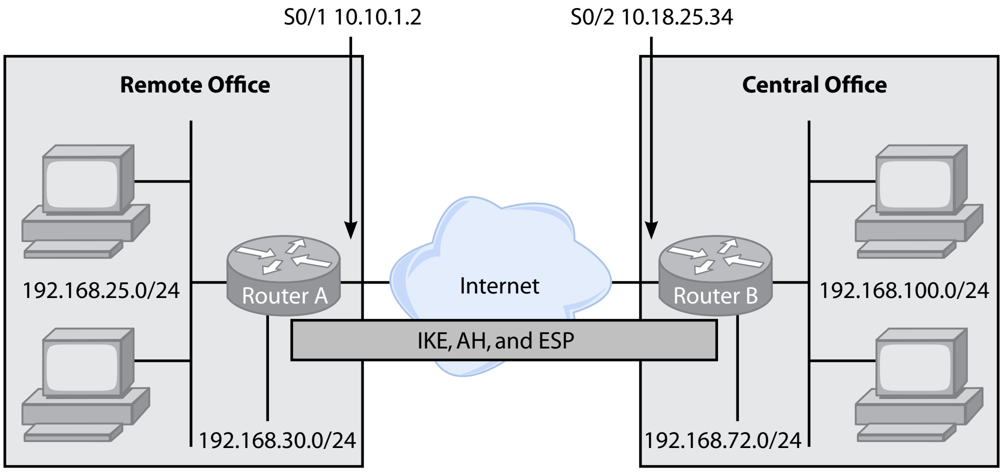
The crypto map command is applied globally to create the map and it is applied to the interface. The name used to create the map must be used on the interface. The static routes applied to each router in Figure 9 allow each side to know about the other.

Step 6: Configure the Interface ACL

With the Interface ACLs you can permit IKE, IPSec packets and IPSec SAs to go through the router. This is important since Internet-facing devices lock most packets destined for the public facing port. Site-to-site IPSec VN tunnels can be between Internet-facing devices.

Since the public IPs applied to each router are generally static, and never changes, the extended access list can be used to allow only traffic from the site-to-site VPN peer. We do not have to allow IPSec packets from all sources and can lock it down to just the other side of the VPN.

Figure 10 shows the access list applied to the interface to allow IPSec traffic.



```
access-list 110 permit ahp host 10.18.25.34 host 10.10.1.2
access-list 110 permit esp host 10.18.25.34 host 10.10.1.2
access-list 110 permit udp host 10.18.25.34 host 10.10.1.2 eq isakmp


Interface serial 0/1
  ip address 10.10.1.2 255.255.255.0
  crypto map to-central
  ip access-group 110 in
```

```
access-list 110 permit ahp host 10.10.1.2 host 10.18.25.34
access-list 110 permit esp host 10.10.1.2 host 10.18.25.34
access-list 110 permit udp host 10.10.1.2 host 10.18.25.34 eq isakmp


Interface serial 0/1
  ip address 10.18.25.34 255.255.255.0
  crypto map to-remote
  ip access-group 110 in
```

Figure 10

The access-list for the internet facing port can be quite large or just deny everything unless it is already established. The three statements in Figure 10 represent the addition of AH, ES and IKE to the already-existing access list. These three lines are also very specific about the source and destination IP addresses that such traffic is permitted through the interface.

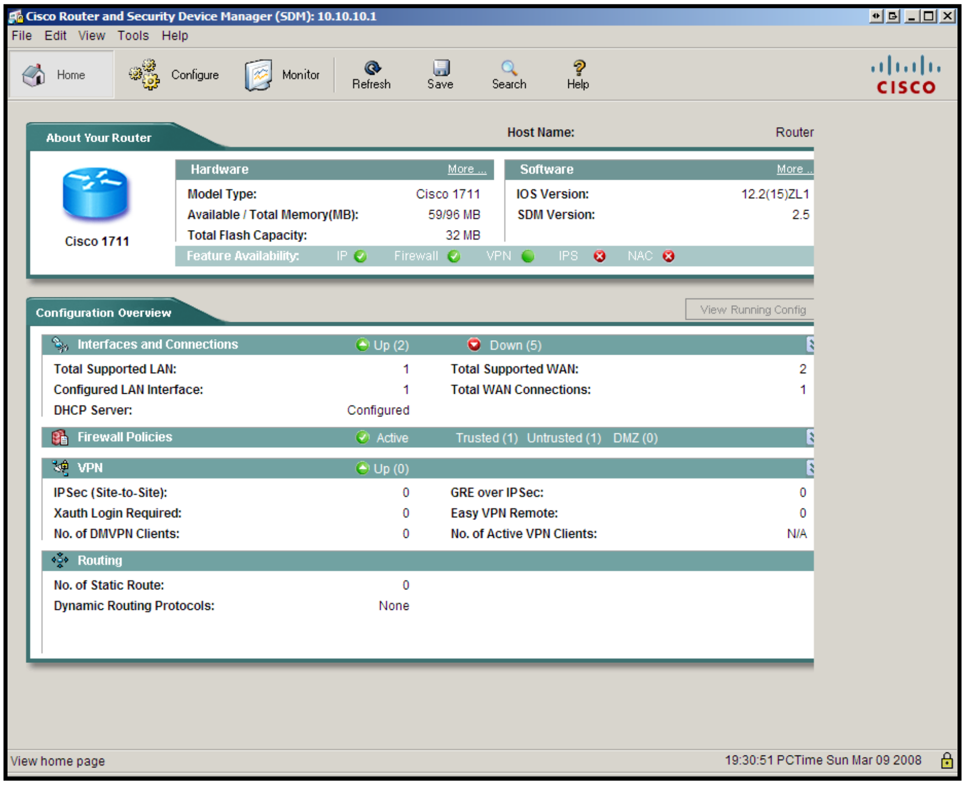
Security Device Manager Features and Interface

SDM is a Cisco web-based configuration tool that permits virtually all IOS features to be configured without accessing the CLI. SDM is embedded in a variety of IOS-based routers such as the 800 through 3800 series routers.

Although SDM does permit many individual IOS options to be configured, the true power of SDM is exhibited through its wizards. These enable rapid configuration of select Cisco access routers. To simplify the installation process, virtually all router configuration tasks have wizards, including:

- Initial router configuration
- Firewall setup
- Site-to-site VPN
- Router lockdown
- Security audit

Figure 11 shows the SDM Home Page.



Host Name: Router

Hardware	
Model Type:	Cisco 1711
Available / Total Memory(MB):	59/96 MB
Total Flash Capacity:	32 MB

Software	
IOS Version:	12.2(15)ZL1
SDM Version:	2.5

Feature Availability: IP ✓ Firewall ✓ VPN ● IPS ☒ NAC ☒

Interfaces and Connections — Up (2) — Down (5)

Total Supported LAN:	1	Total Supported WAN:	2
Configured LAN Interface:	1	Total WAN Connections:	1
DHCP Server:	Configured		

Firewall Policies — Active — Trusted (1) Untrusted (1) DMZ (0)

VPN — Up (0)

IPSec (Site-to-Site):	0	GRE over IPSec:	0
Xauth Login Required:	0	Easy VPN Remote:	0
No. of DMVPN Clients:	0	No. of Active VPN Clients:	N/A

Routing

No. of Static Route:	0
Dynamic Routing Protocols:	None

19:30:51 PCTime Sun Mar 09 2008

Figure 11

- **Home** – Display the hardware, software and configuration overview page
- **Configure** – Provides options to create and edit all router parameters and features
- **Monitor** – Displays configuration and operational status
- **Refresh** – Refreshes the current web page
- **Save** – Saves the current SDM configuration to the router
- **Search** – Allows you to search for key SDM words and features
- **Help** – Provides assistance on how to use SDM

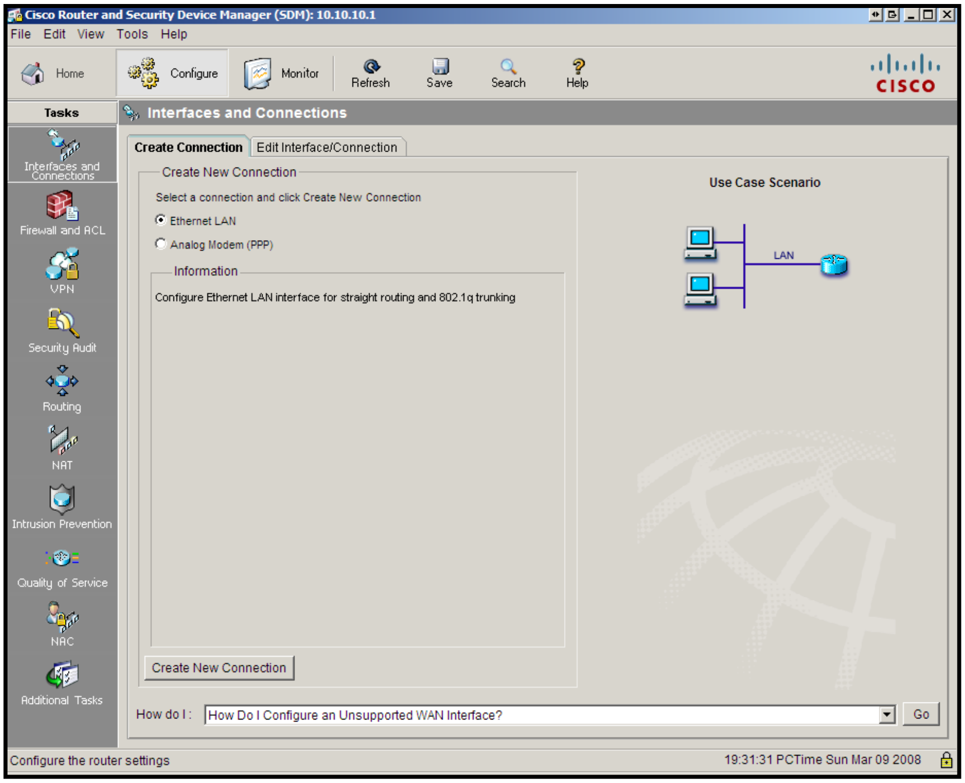
The first section at the top of the SDM page is labeled "About Your Router" and displays information about the router you're connected to. The second section is labeled "Configuration Overview" and lists the following items:

- **Interfaces and Connections** – Shows a count of all LAN and WAN interfaces.
- **Firewall Policies** – Shows trusted, untrusted and DMZ interfaces and which policies are configured and applied.
- **VPN** – Displays account of the number of site-to-site IPSec VPNs, GRE over IPSec tunnels, Xauth clients, DMVPN clients, VPN clients and Easy VPN Remote clients.
- **Routing** – Displays a count of the number of static routes and dynamic routing protocols (if any) configured.
- **Intrusion Prevention** – shows how many signatures the router is aware of and the number of interfaces that IPs is configured on.

By clicking the View Running Config button, this will retrieve a current read-only copy of the CLI configuration.

Configuring a Site-to-Site VPN in SDM

Start by clicking on the Configure button at the top of the screen to display the Configure page. As shown in Figure 12, the left side of the window is the Tasks bar which lists all the configuration options.



Select a connection and click Create New Connection

● Ethernet LAN

○ Analog Modem (PPP)

Configure Ethernet LAN interface for straight routing and 802.1q trunking

How do I : How Do I Configure an Unsupported WAN Interface?

Configure the router settings

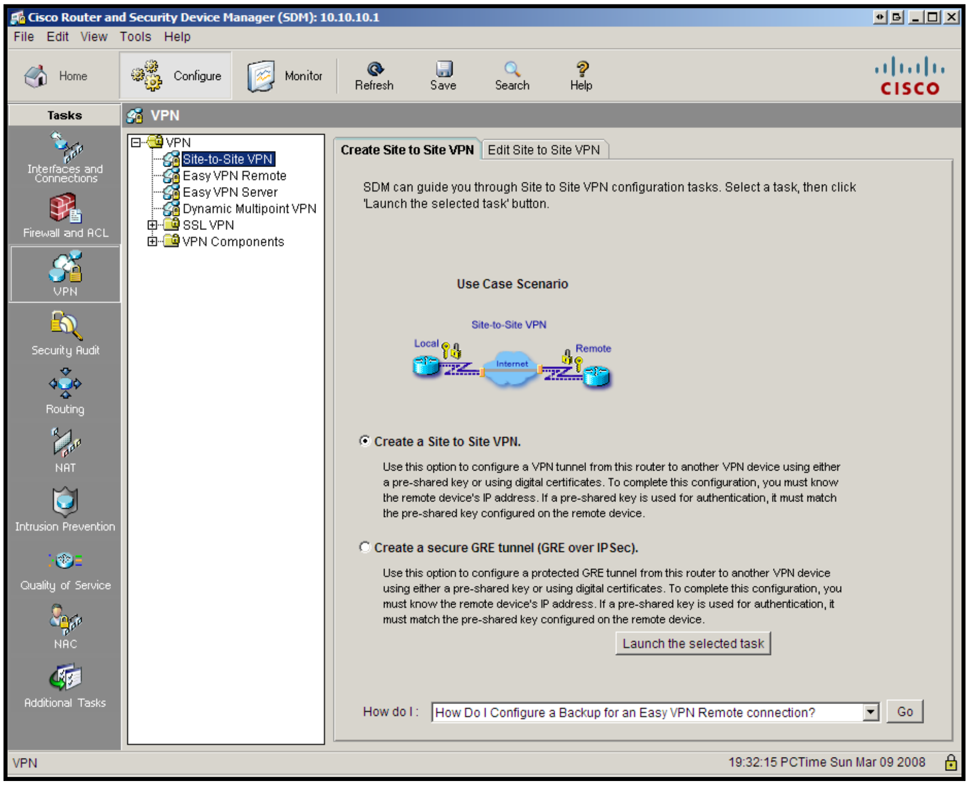
19:31:31 PCTime Sun Mar 09 2008

Figure 12

- **Interfaces and Connections** – Used to create and edit interfaces on the router.
- **Firewall and ACL** – Used to create and edit basic (inside and outside) and advanced (inside, outside and DMZ) firewall configurations in the router.
- **VPN** – Used to create and edit IPSec VPNs, DMVPN and the Easy VPN Remote and Server functions.
- **Security Audit** – Used to perform a security audit of your router and permits a one-step lock-down process to secure the router.
- **Routing** – Used to configure RIP, OSPF and EIGRP on the router.
- **NAT** – Used to configure basic NAT (inside and outside) as well as advanced NAT (inside, outside and DMZ).
- **Intrusion Prevention** – Used to apply network-based intrusion prevention rules to the router and edit them.

- **Quality of Service** – Used to configure LLQ QoS policies for outgoing traffic on both WAN interfaces and IPSec tunnels.
- **NAC** – Used to create and edit Network Access Control policies on the router.
- **Additional Tasks** – Used to configure a variety of other router tasks such as router properties, router access, DHCP, DNS, ACL Editor and AAA.

Click the VPN option on the Tasks bar which gives you five primary VPN configuration options to the right of the Tasks bar as shown in Figure 13 and listed below.



SDM can guide you through Site to Site VPN configuration tasks. Select a task, then click 'Launch the selected task' button.

● Create a Site to Site VPN.

Use this option to configure a VPN tunnel from this router to another VPN device using either a pre-shared key or using digital certificates. To complete this configuration, you must know the remote device's IP address. If a pre-shared key is used for authentication, it must match the pre-shared key configured on the remote device.

○ Create a secure GRE tunnel (GRE over IPSec).

Use this option to configure a protected GRE tunnel from this router to another VPN device using either a pre-shared key or using digital certificates. To complete this configuration, you must know the remote device's IP address. If a pre-shared key is used for authentication, it must match the pre-shared key configured on the remote device.

How do I : How Do I Configure a Backup for an Easy VPN Remote connection?

19:32:15 PCTime Sun Mar 09 2008

Figure 13

- **Site to site VPN** – Launches the Site-to-Site VPN Wizard
- **Easy VPN Remote** – Launches the Easy VPN Remote Wizard
- **Easy VPN Server** – Launches the Easy VPN Server Wizard
- **Dynamic Multipoint VPN** – Launches the Dynamic Multipoint VPN Wizard
- **VPN Components** – Opens a list of individual options for IPSec VPN configuration

Site-to-Site VPN Wizard

By clicking on the Site-to-Site VPN option, this launches the Site-to-Site VPN Wizard. In Figure 13 above, you will see two tabs listed below:

- **Create Site to Site VPN** – Used to create either a new site-to-site VPN or a new GRE over IPSec tunnel.
- **Edit Site to Site VPN** – Used to modify and test an existing site-to-site VPN or GRE over IPSec tunnel.

On the Create Site to Site VPN tab, these two options are available:

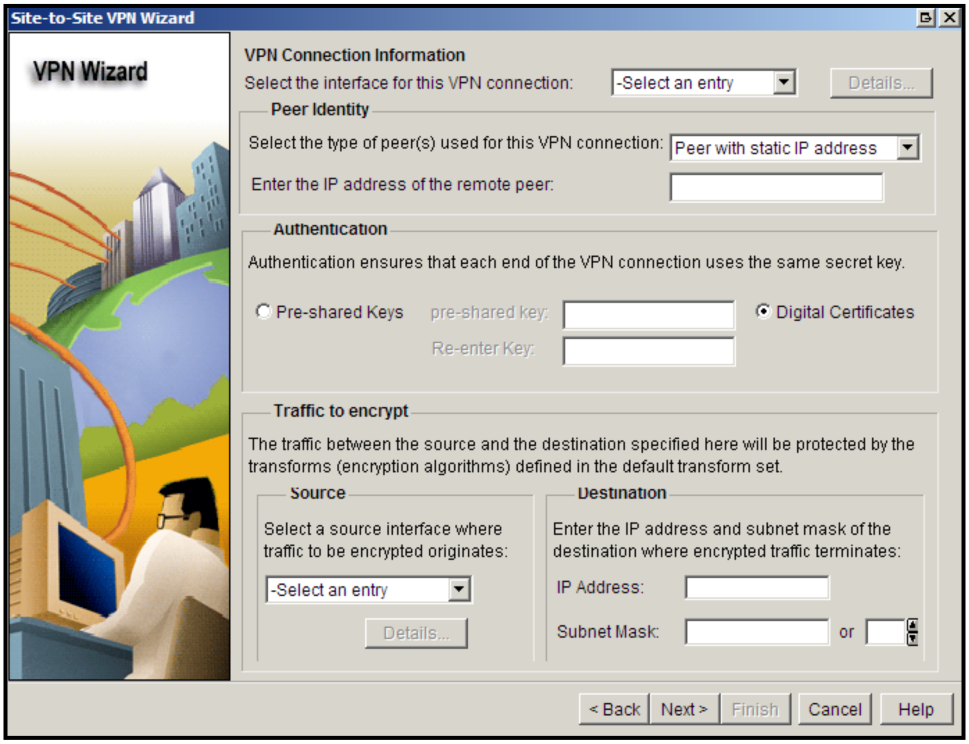
- **Create a Site to Site VPN** – Used to configure an IPSec VPN tunnel from this router to another device.
- **Create a secure GRE tunnel (GRE over IPSec)** – Used to configure a protected GRE tunnel from this router to another device.

Click the **Create a Site to Site VPN** radio button and click the **Launch the selected task** button near the bottom of the screen. The Site-to-Site VPN Wizard window appears and another choice is offered:

- **Quick Setup** – requires minimal information to set up a new IPSec VPN tunnel.
- **Step by Step Wizard** – Permits the use of either a default configuration or a customized configuration for the IPSec VPN tunnel.

Quick Setup

From the Site-to-Site VPN Wizard window, click **Quick Setup** and click the **Next** button. The quick setup option is only one configuration screen followed by a summary screen. Only basic IPSec VPN configuration is possible via the Quick Setup screen. Figure 14 shows the VPN Quick Setup configuration window.



Site-to-Site VPN Wizard

VPN Wizard

VPN Connection Information

Select the interface for this VPN connection: -Select an entry

Peer Identity

Select the type of peer(s) used for this VPN connection: Peer with static IP address

Enter the IP address of the remote peer:

Authentication

Authentication ensures that each end of the VPN connection uses the same secret key.

○ Pre-shared Keys pre-shared key: Re-enter Key: ● Digital Certificates

Traffic to encrypt

The traffic between the source and the destination specified here will be protected by the transforms (encryption algorithms) defined in the default transform set.

Source

Select a source interface where traffic to be encrypted originates: -Select an entry

Destination

Enter the IP address and subnet mask of the destination where encrypted traffic terminates:

IP Address:

Subnet Mask: or

Figure 14

This window offers the following configuration options:

- **VPN Connection Information** – Specify the interface that is the source of the IPSec VPN from this router.
- **Peer Identity** – Specify the type of IP address of the remote peer with the pull-down menu. If you choose Peer with static IP address, you must enter the IP address of the remote peer.
- **Authentication** – Click either **Pre-shared keys** or **Digital Certificates** for IKE authentication. If preshared keys are used, you must enter the key twice for validation.
- **Traffic to encrypt** – Specify which traffic is encrypted and travels through the IPSec VPN and which travels outside the VPN.
    - **Source** – Specify the interface where the encrypted traffic orginates.
    - **Destination** – Specify an IP address or subnet at the remote end of the IPSec VPN connection. The subnet mask or number of bits is used to specify the range of the destination IP addresses.

When finished filling out the quick form, click **Next** at the bottom to proceed to the summary screen where the configured options are displayed. Click **Finish** at the bottom to apply the parameters and complete the configuration. Once this is done, the configuration is pushed to the router.

Step-by-Step Setup

The use of preconfigured parameters in the Quick Setup limits the ability to select specific IKE policies or IPSec transforms or cerate a more robust collection of IP addresses and subnets for interesting traffic. This is the advantage of the Step-by-Step setup with the following four primary tasks described below.

Define Connection Settings

- **VPN Connection Information** – Specify the interface that is the source of the IPSec VPN from this router which is an outside or WAN interface.
- **Peer Identity** – Specify the type of IP address of the remote peer by choosing it from the pull-down menu. You must enter the IP address of the remote peer if you choose Peer with static IP address.
- **Authentication** – Click either **Pre-shared keys** or **Digital Certificates** for IKE authentication.

When finished with the appropriate connection information, click **Next** at the bottom of the screen.

Define IKE Proposals

Only one IKE proposal is needed but the IPSec remote peer must have a duplicate proposal for IKE phase 1 to be successful. However, multiple proposals are typically configured at a central site where many remote locations are peering.

The IKE Proposals screen displays all SDM default IKE proposals and any IKE proposals already configured. You can select a proposal from the list or create a new one by clicking the Add button which allows you to set the following parameters:

- **Priority** – Determines how the new IKE policy is sequenced with existing ones.
- **Encryption** – Select the appropriate encryption algorithm (DES, 3DES or AES).
- **Hash** – Select the appropriate hash algorithm (MD5 or SHA-1).
- **D-H Group** – Select the appropriate Diffie-Hellman group (1, 2 or 5).
- **Authentication** – Select the authentication method (preshared key or RSA signatures).
- **Lifetime** – Enter hours, minutes and seconds for the IKE lifetime.

When you have finished entering the new parameters, click the **OK** button and the new IKE proposal appears sequenced according to its priority number. When you are done entering all IKE proposals click **Next** at the bottom of the screen.

Define IPSec Transform Sets

As with IKE proposals, only one IPSec transform set is needed but the IPSec peer must have a duplicate transform set for IKE phase 2 to be successful. Multiple transform sets are typical at a central site with many remote locations peering.

The IPSec Transform Set screen displays the selected transform set that is used with this IPSec VPN. You can select a transform set from the list or create a new one by clicking the Add button which opens the Add Transform Set window. The settings are as follows:

- **Name** – Provide a local name for this transform set that is inserted into the crypto map.
- **Data Integrity with Encryption (ESP)** – Check this box if you wish to use ESP. You must select an identify algorithm (an authentication HMAC, either MD5 or SHA-1) and an encryption algorithm (DES, 3DES or AES).
- **Data and Address Integrity Without Encryption (AH)** – Check this box if you wish to use AH and select an identity algorithm (an authentication HMAC, either MD5 or SHA-1).
- **Mode** – Select either Tunnel, which protects both the data and the IP header, or Transport, which protects only the data.
- **IP Compression** – Check this box if you optionally want to use Comp-LZS compression through the IPSec VPN.

When finished entering the new parameters, click the **OK** button and the new IPSec transform set appears in the list. Click **Next** at the bottom of the screen and the transform set is applied to the IPSec connection.

Define the Traffic to Protect

You can either match a single IP address/subnet on each end of the IPSec VPN or use an access list to perform more advanced interesting traffic matches.

If you need to only protect a single IP address or subnet on both ends, click the **Protect all traffic between the following subnets** radio button. Enter an IP address or subnet and associated mask in the Local Network portion of the screen. This is typically a subnet directly attached to the router but does not have to be. You will also enter an appropriate IP address or subnet with mask in the Remote Network portion of the screen. When finished, click the **Next** button to view the summary page.

To use an ACL to specify interesting traffic, click the **Create/Select an access-list for IPSec traffic** radio button. This has two different fulfillment paths. One is to select an existing ACL and the other is to create a new ACL from scratch. If you want to select an existing ACL, click the **…** pull-down button and choose the **Select an existing rule (ACL)** option. Highlight the existing ACL and click the **OK** button at the bottom to return to the Traffic to Protect screen.

If you want to create a new ACL, click the **…** pull-down button and choose **Create a new rule (ACL)** option which launches the Add a Rule window. Enter a name or number for the new ACL rule. Remember, extended access-list numbers should be between 100 and 199 inclusive. The name can be any alphanumeric combination you desire. You can, optionally, enter a description for the new rule. Click the **Add** button which will open the Add an Extended Rule Entry window. Each entry for this new access list is created with this window. If you have five subnets that need to be protected via the IPSec VPN, you must visit this window five times which adds a new line from the Add a Rule window.

Since ACLs are processed top-down, specific subnets and hosts must be defined at the top of the list. If a generic statement is at the top, this nullifies any specific statements further down the list. General ACL creation rules apply: source and destination IPs/subnets, wildcard masks, specific IP protocols or specific ports.

When finished with this one rule, click the **OK** button to return to the Add a Rule window. If you have other subnets or IP addresses to add to the list, click the **Add** button to add another line to the list. Click the **OK** button at the bottom of the window to continue.

Complete the Configuration

Since all four tasks are now complete, the configuration is displayed. The Summary screen has the same format as the one displayed after the Quick Setup. However, you have the choice to modify the options during the step-by-step setup. If you notice a configuration error, you can navigate back to the appropriate portion of the wizard to correct the mistake.

When the configuration appears complete and correct, click the **Finish** button and the configuration is pushed to the router. Click the **OK** button to continue and return to the Edit Site to Site VPN tab of the Site-to-Site VPN Wizard.

Testing the IPSec VPN Tunnel

Click the **Edit Site to Site VPN** tab at the top of the window and select the VPN you wish to test. There must be a remote peer configured with this router to test the connection. If there is, click the **Test Tunnel** button at the bottom of the screen. If all of the parameters are correct the tunnel should become active. Since the tunnel does not become active until there is interesting traffic being sent, the Test Tunnel option forces the tunnel negotiation process to start.

To create an IOS configuration that is an appropriate mirror of the IPSec VPN tunnel that is highlighted, click the **Generate Mirror** button at the bottom of the screen. This is useful if the remote router does not have SDM installed.

Monitoring the IPSec VPN Tunnel

In SDM, click the Monitor button at the top of any SDM screen to enter the page. The options you have on the left are:

- **Overview** – Displays a generic status of the router, including CPU and memory usage, as well as an overview of the interfaces, firewall, QoS, VPN and logs
- **Interface Status** – Allows the ability to monitor live traffic or test the interfaces
- **Firewall Status** – Displays a log of packets denied by the firewall
- **VPN Status** – Displays a status of IPSec tunnels, DMVPN tunnels, the Easy VPN Server and IKE SAs
- **QoS Status** – Displays the effects of the QoS interface configuration
- **NAC Status** – Displays the number of NAC sessions for both the router and the interfaces
- **Logging** – Displays the buffered log of the router

By clicking the **VPN Status** button in the Tasks bar, you are taken to the VPN Status screen. Here you will see the current status of each IPSec VPN and a count of all packets that have navigated each VPN. You also have the Test Tunnel button which does the same as above.

There are two primary commands to monitor the current status of all IPSec VPNs. The **show crypto isakmp sa** command displays all active IKE sessions; this is phase 1. A QM_IDLE state indicates the IKE SA is active and operational. The **show crypto ipsec sa** command shows all IPSec SAs; this is phase 2. A successful IPSec SA is indicated by non-zero counts of encrypted and decrypted packets.

The entire IKE process can also be debugged using the **debug crypto isakmp** command which shows the IKE profile and IPSec transform set negotiations during the two IKE phases, 1 and 2.

GRE Tunneling over IPSec

GRE, generic routing encapsulation, tunnels have been around for quite some time. First developed by Cisco, it's a means to carry other routed protocols across a predominately IP network. The primary use of GRE was to carry non-IP packets through an IP network and was also used to carry IP packets through an IP cloud. The generic characteristics of a GRE tunnel are:

- 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 Cisco IOS Software Release 12.4(4)T.
- GRE has relatively weak security features.

A GRE tunnel is similar to an IPSec tunnel in that the tunnel has two endpoints. Traffic enters one end of the tunnel and exits the other end and, while in the tunnel, routers use the new outer header only to forward the packets. Unlike an IPSec tunnel, the GRE tunnel is stateless, meaning 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. GRE permits routing protocols (such as OSPF and EIGRP) across the connection, which is not the case with a typical IPSec tunnel.

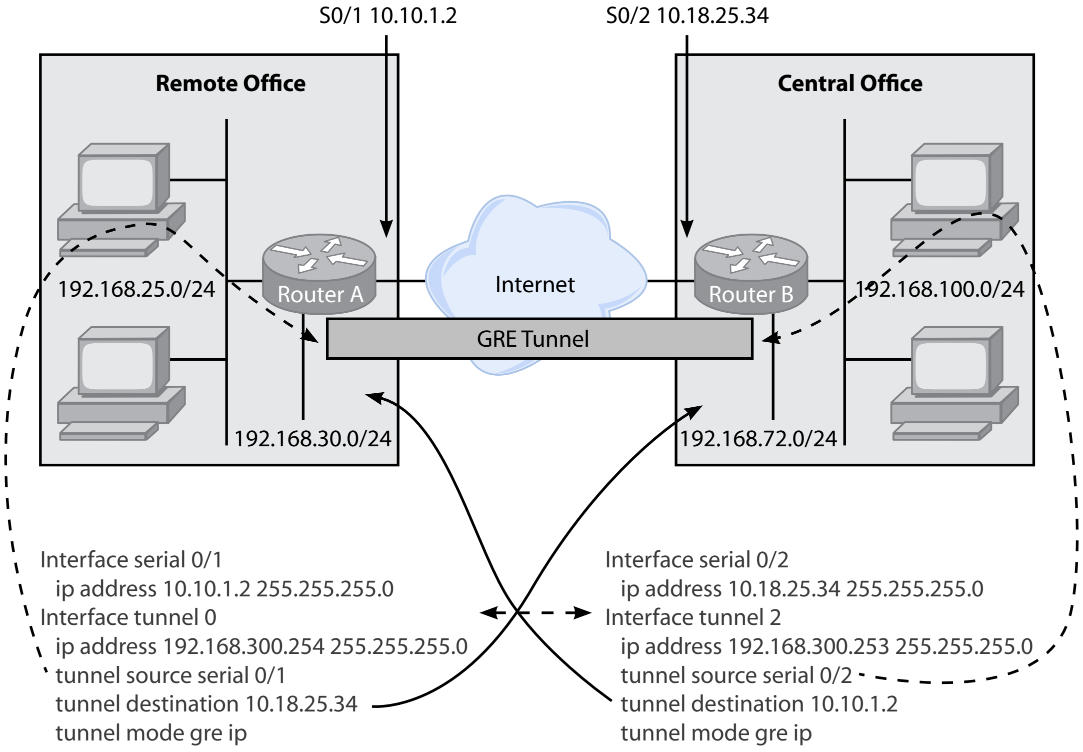
The GRE header contains 4 bytes which represent the minimum size of GRE header with no added options. The first pair of bytes (bits 0 through 15) contains the flags that indicate the presence of GRE options. If active, they add additional overhead to the GRE header. The second pair of bytes is the protocol field and indicates the type of data that is carried in the GRE tunnel. Table 21 describes the 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.

Table 21

Basic GRE Configuration

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 15 shows a basic GRE tunnel setup.



```
Interface serial 0/1
  ip address 10.10.1.2 255.255.255.0
Interface tunnel 0
  ip address 192.168.300.254 255.255.255.0
  tunnel source serial 0/1
  tunnel destination 10.18.25.34
  tunnel mode gre ip
```

```
Interface serial 0/2
  ip address 10.18.25.34 255.255.255.0
Interface tunnel 2
  ip address 192.168.300.253 255.255.255.0
  tunnel source serial 0/2
  tunnel destination 10.10.1.2
  tunnel mode gre ip
```

Figure 15

The basic configuration includes:

- 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

Secure GRE Tunnels

"GRE over IPSec" implies the GRE packet sits higher in the stack than the IPSec portion. The original packer is the innermost layers then the GRE wrapper appears. Finally, the IPSec portion is added for security. Figure 16 shows the GRE over IPSec packet format.

Tunnel Mode

ESP IP Header	ESP Header	GRE IP Header	GRE	IP Header	TCP Header	Data	ESP Trailer

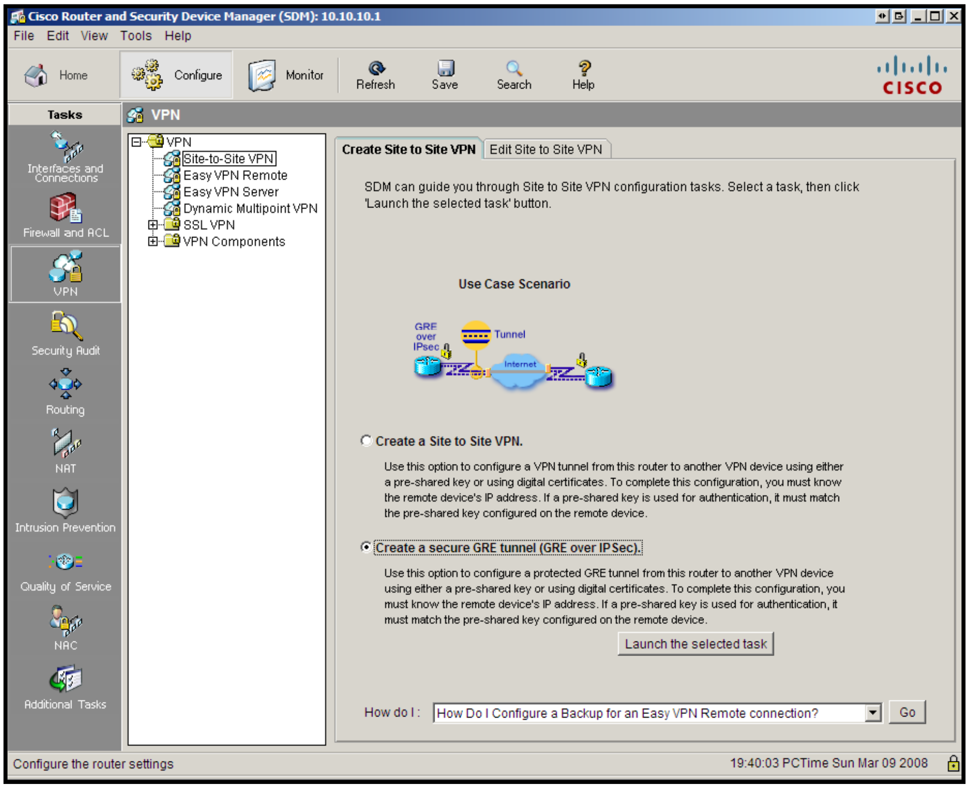
Transport Mode

GRE IP Header	ESP Header	GRE	IP Header	TCP Header	Data	ESP Trailer

Figure 16

Configure GRE Over IPSec Using SDM

Configuring the GRE tunnel is done in the same screen as configuring a site-to-site VPN. As shown in Figure 17, click the **Configure** button on the menu bar; click **VPN** on the left most navigation bar; click **Site-to-Site VPN** on the next menu bar to the right; select **Create a secure GRE tunnel** and click **Launch the selected task**.



SDM can guide you through Site to Site VPN configuration tasks. Select a task, then click 'Launch the selected task' button.

○ Create a Site to Site VPN.

Use this option to configure a VPN tunnel from this router to another VPN device using either a pre-shared key or using digital certificates. To complete this configuration, you must know the remote device's IP address. If a pre-shared key is used for authentication, it must match the pre-shared key configured on the remote device.

● Create a secure GRE tunnel (GRE over IPSec).

Use this option to configure a protected GRE tunnel from this router to another VPN device using either a pre-shared key or using digital certificates. To complete this configuration, you must know the remote device's IP address. If a pre-shared key is used for authentication, it must match the pre-shared key configured on the remote device.

How do I : How Do I Configure a Backup for an Easy VPN Remote connection?

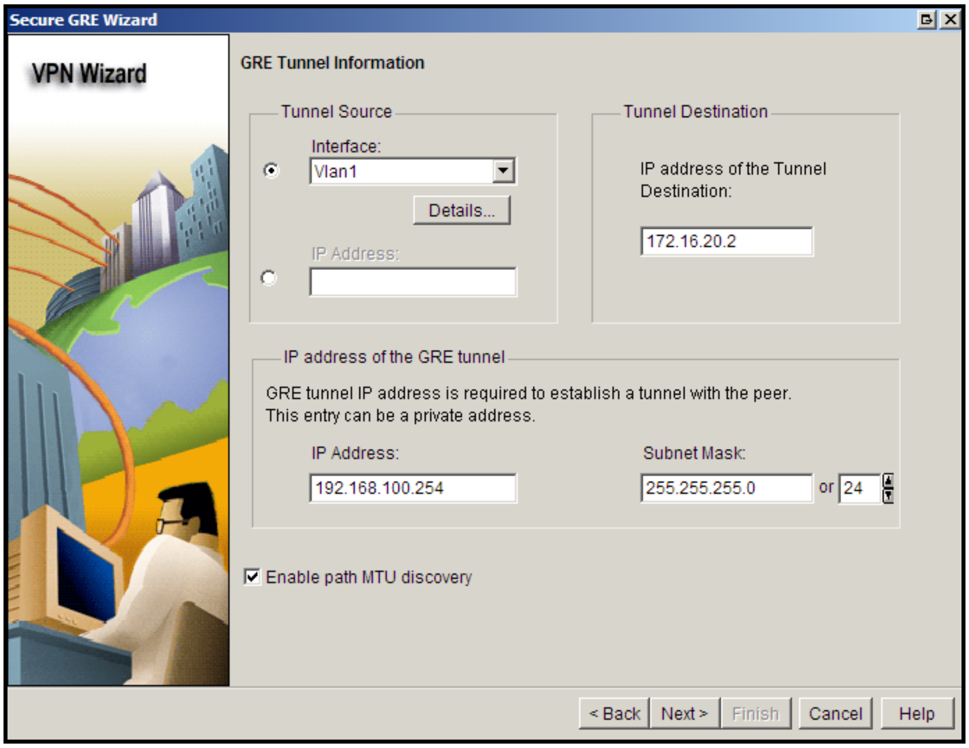
Configure the router settings

19:40:03 PCTime Sun Mar 09 2008

Figure 17

Step 1: Create the GRE Tunnel

There are two sets of IP addresses that are applied to the GRE tunnel interface – the tunnel source and destination. The source is selected either from the pull-down list of interfaces or entered manually. If an interface is selected for the source, the GRE tunnel will use the IP address of that interface. The tunnel destination is the IP address of the remote GRE peer and must be manually entered. When you are finished, click **Next** at the bottom of the window, shown in Figure 18.



GRE Tunnel Information

Tunnel Source

● Interface: Vlan1

○ IP Address:

Tunnel Destination

IP address of the Tunnel Destination: 172.16.20.2

IP address of the GRE tunnel

GRE tunnel IP address is required to establish a tunnel with the peer. This entry can be a private address.

IP Address: 192.168.100.254

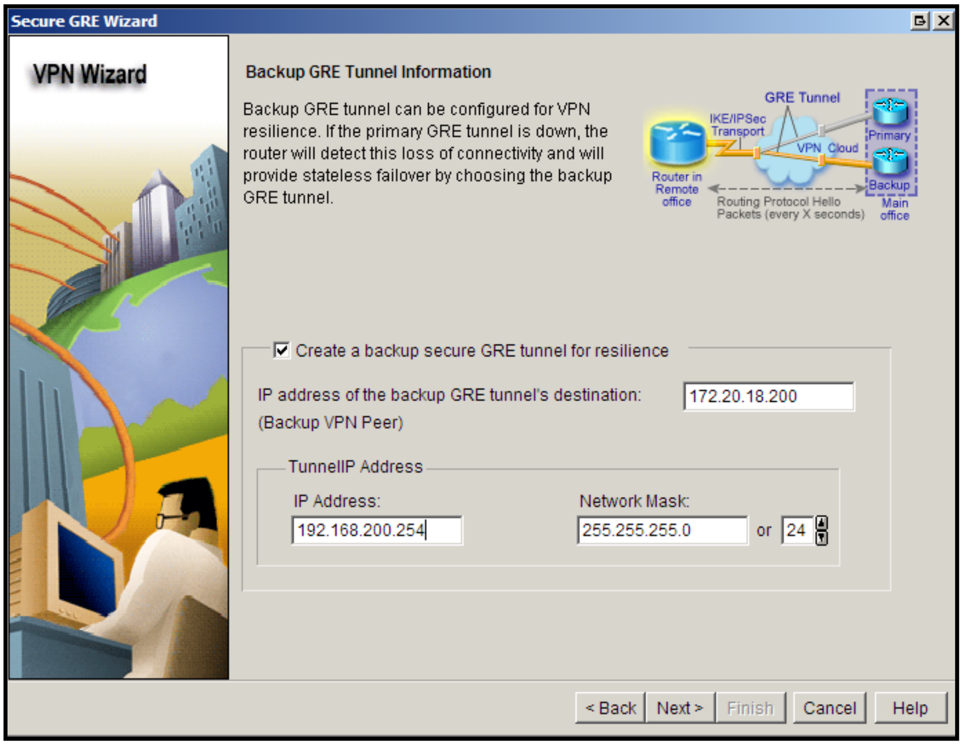
Subnet Mask: 255.255.255.0 or 24

☑ Enable path MTU discovery

Figure 18

Step 2: Create a Backup GRE Tunnel

By using the wizard to create the GRE tunnel, you can create a second GRE tunnel for survivability. If the tunnel fails for some reason, then the IPSec tunnel that is carried within it fails also. A backup provides stateless failover in the event the primary GRE tunnel fails. Since a GRE tunnel is an optional feature, you must check the **Create a backup secure GRE tunnel for resilience** box to activate the window. The configuration options are similar to those used to create the primary tunnel. The tunnel source is the same as the primary so you don't have an option to select the source. You will have to provide an alternate destination peer for the backup tunnel. Figure 19 shows the backup screen.



Secure GRE Wizard

VPN Wizard

Backup GRE Tunnel Information

Backup GRE tunnel can be configured for VPN resilience. If the primary GRE tunnel is down, the router will detect this loss of connectivity and will provide stateless failover by choosing the backup GRE tunnel.

☑ Create a backup secure GRE tunnel for resilience

IP address of the backup GRE tunnel's destination: 172.20.18.200
(Backup VPN Peer)

TunnelIP Address

IP Address: 192.168.200.254

Network Mask: 255.255.255.0 or 24

Figure 19

Like the primary GRE tunnel, you must create a unique IP address on a new subnet within the backup tunnel. The remote peer must use the same subnet with an exclusive address of its own. When finished, click **Next** at the bottom of the window.

Steps 3-5: IPSec VPN Information

Since the IPSec tunnel is the outermost layer of the GRE tunnel, you need to enter the IPSec information for the GRE tunnel to travel across.

The first step is to enter the VPN authentication information by selecting either digital certificates or pre-shared keys. Remember, if pre-shared keys are used you need to enter them twice.

The second step is to select or create the IKE proposals. The windows are identical to creating IKE proposals in the site-to-site VPN wizard. Remember, the remote peer must have an identical IKE proposal configured for the tunnel to work and can be used for many remote peers.

The third step is to select or create IPSec transform sets. This window is identical to creating the IPSec transform sets in the site-to-site VPN wizard. New transform sets can be created and the appropriate transform set can be selected for use with the IPSec VPN. Again, the remote peer must have an identical IPSec transform set configured and can be used for many remote peers.

Step 6: Routing Information

Once the GRE and IPSec tunnels have been configured, a routing protocol needs to be selected to traverse the GRE tunnel. The only routing option with a typical IPSec VPN is static routes. This has to be configured on each end and only determines which prefixes are reachable through the IPSec VPN.

Static routing is the default option in the routing protocol selection process and there are three other routing options within the GRE tunnel window:

- EIGRP
- OSPF
- RIP

Static Routes

To support small stub sites that only have a single subnet, static routing is typically used. No dynamic routing information is exchanged between sites. If a site has multiple subnets which use the VPN or if a site uses a backup VPN tunnel, then static routing is not appropriate.

If static routing is selected, you are given a choice to do split tunneling or not. Split tunneling allows you to send some traffic through the tunnel and the remainder of the traffic through the Internet. This allows you to access the services on the other side of the tunnel but use your local Internet connection to avoid overtaxing the tunnel.

RIP

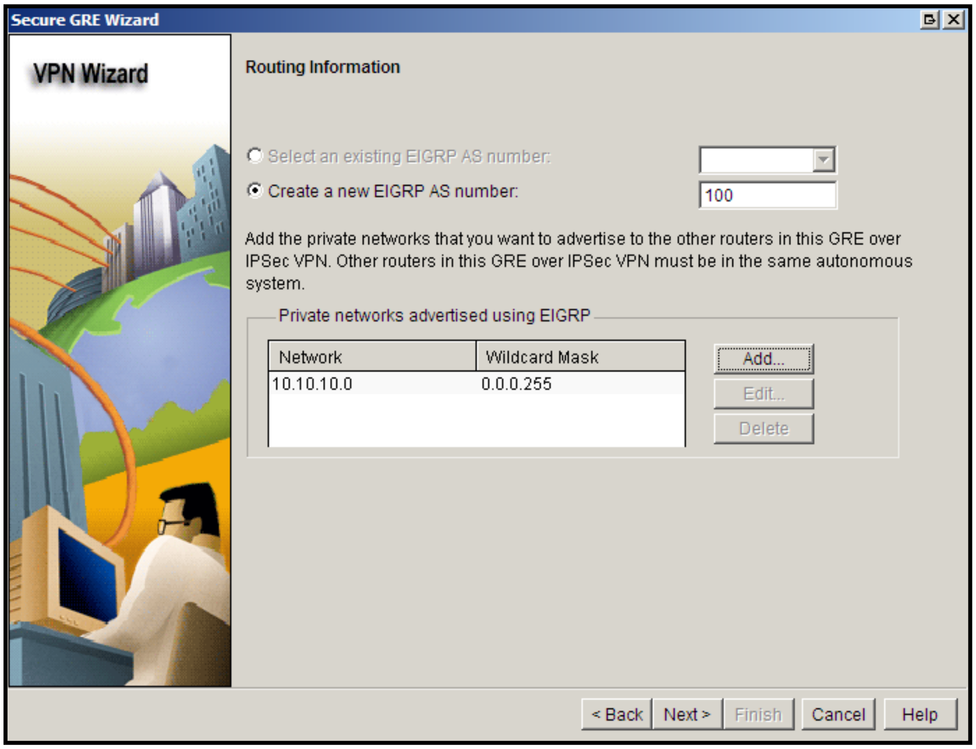
You will have two selections for RIP, RIP version 1 and RIP version 2. RIP version 1 is the older classful version and RIP version 2 allows classless subnets and sends the subnet mask with the routing updates. You can add only whole classful network numbers to RIP and all subnets of that network number are included. Also, you must add the IP subnet of the GRE interface for RIP to use the interface. Traffic that you want protected by the VPN will need to be added to the RIP configuration. Traffic outside of the RIP routes avoids the VPN.

OSPF

In order to use OSPF, you have to create an OSPF process ID. If OSPF is already configured on the router, you can select the process ID from the pull-down menu. If you have to create a process ID, you must determine the OSPF area ID to be used in the GRE over IPSec tunnel. To add local networks to the OSPF routing protocol, you must enter a subnet number, wildcard mask and an area for each network. Additionally, you must add the IP subnet/mask/area of the GRE interface for OSPF to use the interface. Like RIP, only traffic in the exchanged routes is protected by the VPN.

EIGRP

First, select or create an EIGRP autonomous system (AS) number. Like OSPF, if EIGRP is already in use on the router, you can select the AS number from the pull-down menu. If not, you must create a new AS number in the router. For EIGRP, you must enter a subnet number and a wildcard mask for each network. You must also add the IP subnet/mask of the GRE interface for EIGRP to use it. Like the other routing protocols, traffic outside the EIGRP routes being exchanged will not traverse the tunnel and be unprotected. Figure 20 shows the Routing Information screen for EIGRP.



Routing Information

○ Select an existing EIGRP AS number:

● Create a new EIGRP AS number: 100

Add the private networks that you want to advertise to the other routers in this GRE over IPSec VPN. Other routers in this GRE over IPSec VPN must be in the same autonomous system.

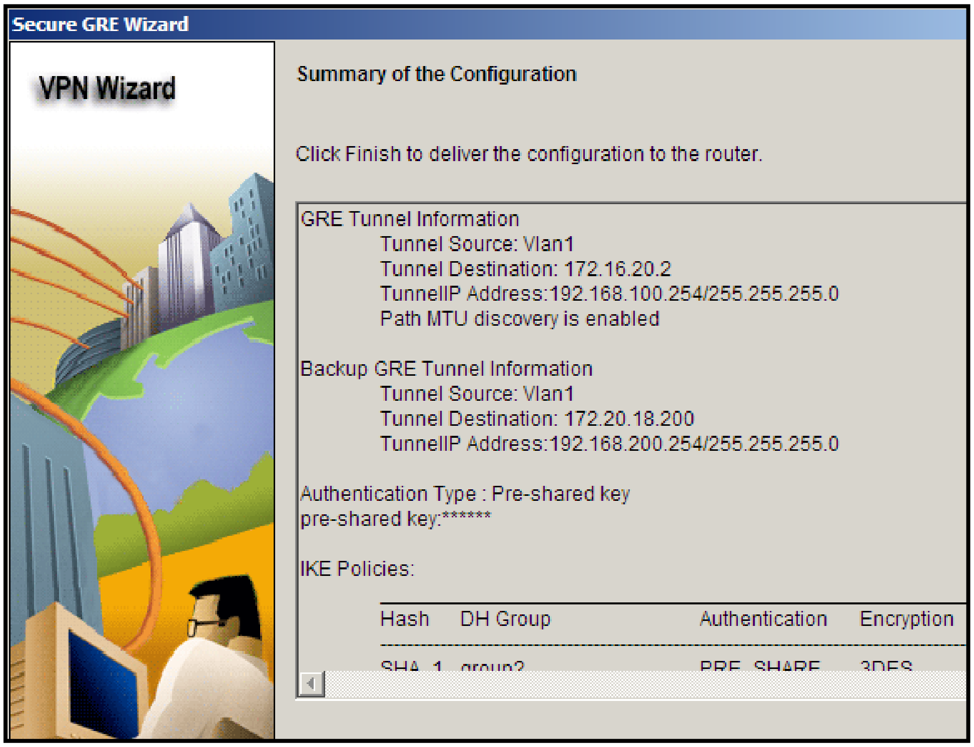
Private networks advertised using EIGRP

Network	Wildcard Mask
10.10.10.0	0.0.0.255

Figure 20

Step 7: Validate the GRE over IPSec Configuration

Once the routing protocol is selected and configured, you are brought to the Summary of Configuration window. You will probably need to use the scroll bar to see the entire configuration. Look through the configuration to ensure everything is correct. If not, use the **Back** button to go back and correct the errors. Figure 21 shows the summary screen.



Summary of the Configuration

Click Finish to deliver the configuration to the router.

```
GRE Tunnel Information
          Tunnel Source: Vlan1
          Tunnel Destination: 172.16.20.2
          TunnelIP Address:192.168.100.254/255.255.255.0
          Path MTU discovery is enabled

Backup GRE Tunnel Information
          Tunnel Source: Vlan1
          Tunnel Destination: 172.20.18.200
          TunnelIP Address:192.168.200.254/255.255.255.0

Authentication Type : Pre-shared key
pre-shared key:******

IKE Policies:

          Hash     DH Group                Authentication     Encryption
          ---------------------------------------------------------------
          SHA_1    group2                  PRE_SHARE          3DES
```

Figure 21

IPSec High Availability Options

Since an IPSec VPN is an end-to-end connection, there are a number of possible points that are vulnerable to failure.

An access link failure could be the physical interface, or a module containing the interface, on any transit network device. This could also include the cable that provides transport, electrical, optical or wireless.

It can be difficult to determine the exact cause of the failure of a rempote peer unless you have some network management reachability in the remote site.

For a device failure, this could include any device between and including the source and destination of the VPN. In many cases, these devices are beyond your administrative control and cause of the failure cannot be determined.

If it is a routing or circuit issue in a network between the endpoints, this would be a path failure. This is, like a device failure, typically outside your administrative reach and cannot easily be determined.

Failure Mitigation

Each of the failure sources above can be mitigated by employing one or more redundancy mechanisms.

- **Access link failure** – Multiple interfaces and devices can be used. A single endpoint could have multiple interfaces, multiple interface cards or multiple endpoint devices.
- **Remote peer failure** – This can be mitigated in a similar manner by using multiple interfaces and devices to survive a failure.
- **Device failure** – Again, duplicate interfaces and devices can help overcome a local failure. If a device failure is outside of your administrative control, this could be a challenge to correct. To alleviate, or reduce, this circumstance, ensure that you have multiple diverse paths between endpoints.
- **Path failure** – This is typically beyond your control. Path redundancy can be used to circumvent a path failure in an untrusted network.

To achieve path redundancy, you need to consider what is truly required. Any single point of failure should be removed from the path. This would mean, within your network, duplicate equipment and wiring and also imply separate and diverse paths into and out of the building. To achieve this, the use of different IPSs ensures the traffic starts in different pieces of the Internet. However, it is difficult to ensure that a common circuit from an upstream ISP is not used "somewhere" between endpoints.

Failover Strategies

If the failure state cannot be recognized then the best redundancy plans cannot be executed. IPSec failover can be executed in two ways.

- **Stateless** – Redundant logical VPN tunnels are used to provide the primary and backup paths. Use of the paths is determined by message exchanges between peers or a determination by the end devices on which path to use. If the end-to-end path has failed, the traffic is sent across the backup tunnel since the *state* of the tunnel is not known.
- **Stateful** – This strategy employs redundant equipment which means the devices used to provide stateful failover are typically identical. This includes configuration, interfaces, operating system and so on. To determine the best current device, they communicate with each other.

IPSec Stateless Failover

There are three primary stateless means to detect and react to a failure, to determine this.

Dead Peer Detection

Dead peer detection is a configurable option during the IPSec VPN setup. It also offers a stateless failover from one tunnel to another and the routers are not keeping track of which tunnel is currently active. Instead, a secondary tunnel is selected when traffic flowing through the primary tunnel fails. There are two operational modes: periodic and on-demand.

The DPD periodic mode has the following characteristics:

- DPD keepalive messages are periodically sent between peers.
- DPD keepalive messages are in addition to normal IPSec rekey messages that also traverse the tunnel.
- DPD keepalive messages are not sent if user data is transmitted through the tunnel.
- DPD keepalive messages are used only when there is a lull in traffic across the tunnel.

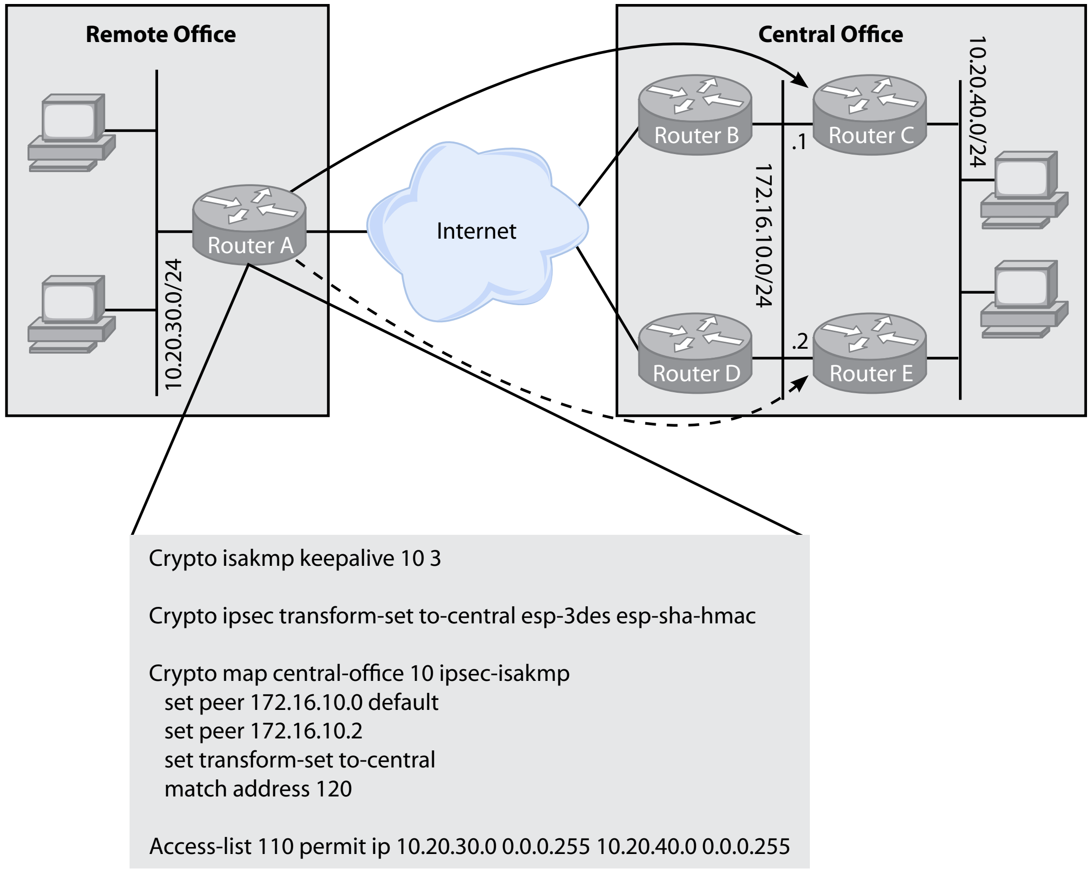
One downside of periodic DPD mode is the potentially excessive tunnel overhead. The IPSec SA rekeying messages which occur as the IPSec lifetime nears expiration already regularly pass through the tunnel. Even though the keepalive messages add more encryption/decryption overhead to the VPN endpoints, the addition of these messages provides more timely failure detection.

The DPD on-demand mode has the following characteristics:

- This is the default mode in a Cisco IOS device.
- DPD keepalive messages are sent only if the liveliness of the peer is in question. A response is expected if traffic is sent to the peer. If the response does not arrive, a DPD keepalive message is sent.
- DPD keepalive messages are never sent during otherwise idle tunnel moments.
- The discovery of a dead peer might not occur until the IKE or IPSec SA rekey is attempted.

On-demand reduces the additional tunnel overhead, however; an alternate tunnel might not be used immediately upon failure. If there is no traffic flowing through the tunnel and it fails, then there is no need to change to an alternate tunnel until user data arrives.

The **crypto isakmp keepalive** command determines the mode and frequency of DPD. As listed above, **periodic** mode sends DPD keepalive messages which are continually sent to verify if the peer is alive. **On-demand** mode is the default and only sends DPD messages if the remote peer is believed to be dead. There are two timer options, *seconds* and *retries*. The **seconds** option determines how often keepalive messages are sent in periodic mode and the **retries** option determines how long to wait to resend DPD messages after the previous one has failed.



```
Crypto isakmp keepalive 10 3

Crypto ipsec transform-set to-central esp-3des esp-sha-hmac

Crypto map central-office 10 ipsec-isakmp
  set peer 172.16.10.0 default
  set peer 172.16.10.2
  set transform-set to-central
  match address 120

Access-list 110 permit ip 10.20.30.0 0.0.0.255 10.20.40.0 0.0.0.255
```

Figure 22

In Figure 22, the primary peer is indicated with the **default** option. This peer is initially used between the remote and central offices. The secondary peer, 172.16.10.2, is not used unless DPD determines the primary peer has failed.

IGP within a GRE over IPSec Tunnel

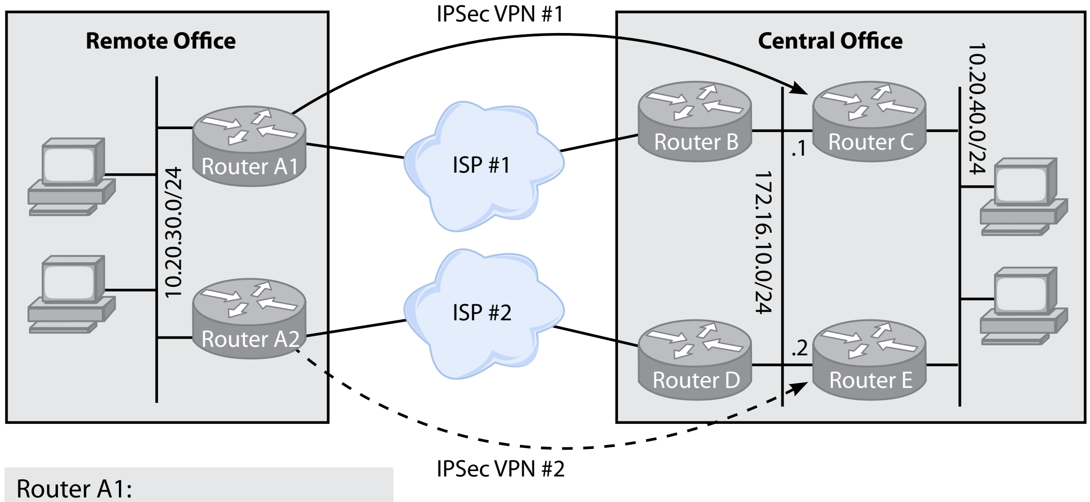
Even though OSPF and EIGRP have very fast convergence around failed links and the use of a backup GRE tunnel does provide redundancy, this does so at the cost of additional IGP overhead in the VPN tunnel. With two or more GRE tunnels connecting two sites, the IGP that runs across the tunnels makes very rapid routing decisions on alternative paths. However, ensuring there is no single point of failure in the paths is important. If all tunnels start on one router and end on a different router, the failure of either router eliminates all tunnels.

HSRP

Generally, hosts are configured with a single default gateway either statically or dynamically. If the gateway fails, the hosts become isolated. Using more than one gateway becomes costly and adds complexity to the network. HSRP can be implemented which utilizes a logical gateway with multiple physical routers. By using HSRP, you do not have to configure multiple gateway addresses on each host since failover could take some time if the main gateway fails.

The HSRP group handles the traffic destined for the logical gateway IP address. The active router handles all packets destined for the logical IP address and a standby router exists to forward packets only if the active router fails.

There can be any number of routers in an HSRP group but a large number can become impractical. There is only one active router per group and the remaining routers in the group elect the standby router. The two routers communicate with each other, which is how the standby router will know the active router has failed.



Router A1:

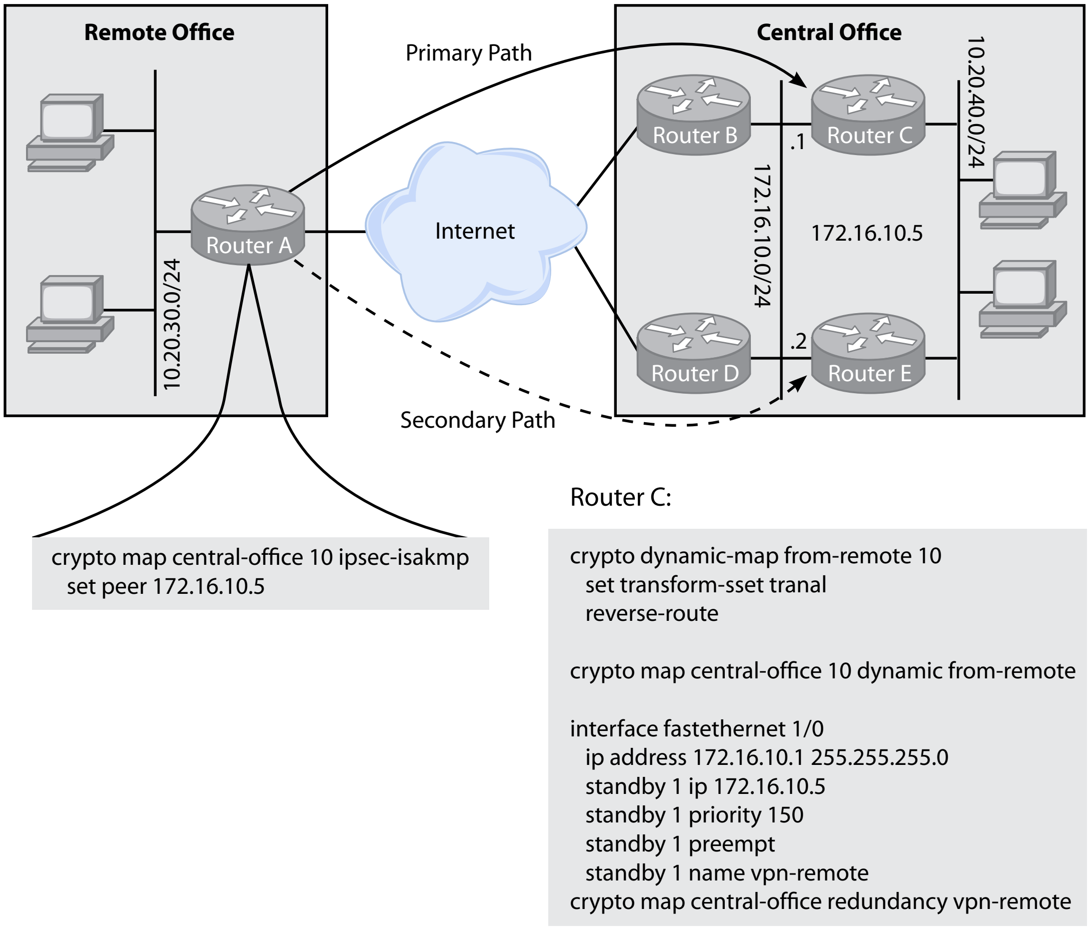
```
interface fastethernet 0/1
  ip address 10.20.30.1 255.255.255.0
  standby 1 ip 10.20.30.5
  standby 1 priority 150
  standby 1 preempt
```

Router A2:

```
interface fastethernet 0/1
  ip address 10.20.30.2 255.255.255.0
  standby 1 ip 10.20.30.5
```

Figure 23

As shown in Figure 23, hosts at the remote office would use 10.20.30.5 as the default gateway, which is the HSRP group IP address between routers A1 and A2. The active router, initially, is Router A1 which is configured with a higher HSRP priority (default is 100). If Router A1 ever fails and comes back to life, the **preempt** command says that if it has a higher priority, it will regain active HSRP. HSRP does not interact with the VPN configuration since HSRP simply selects the active default gateway.



```
crypto map central-office 10 ipsec-isakmp
  set peer 172.16.10.5
```

Router C:

```
crypto dynamic-map from-remote 10
  set transform-sset tranal
  reverse-route

crypto map central-office 10 dynamic from-remote

interface fastethernet 1/0
  ip address 172.16.10.1 255.255.255.0
  standby 1 ip 172.16.10.5
  standby 1 priority 150
  standby 1 preempt
  standby 1 name vpn-remote
crypto map central-office redundancy vpn-remote
```

Figure 24

In Figure 24, HSRP is configured between routers C and E for the VPN connections, and not the hosts, and they are the headend for all remote sites since the 172.16.10.0/24 subnet is reachable globally. The remote site uses 172.16.10.5 as its peer and at the central office. This IP address is the virtual group IP between routers C and E. However, the remote does not benefit from the redundancy. The configuration listed is for Router C but would be identical on Router E. An HSRP group can be configured on the LAN side of Routers C and E to provide redundancy for the hosts.

The interface **crypto map** statement indicates the HSRP group **vpn-remote** provides redundancy and the group name is defined on the interface. Since the central office is configured with a dynamic crypto-map, any remote office can initiate a VPN connection with the central office. This makes it possible for remote offices that have DSL or another connection without static external addresses to connect to the VPN.

If Router C is active and fails, the tunnel will drop as well. The remote will reestablish a tunnel to the same peer IP address which is then handed off to Router E. When Router C comes back up, the tunnel again drops, the remote will reestablish a tunnel with the peer and it is handed off to Router C.

IPSec Stateful Failover

Stateful failover typically needs a set of identical equipment so failover can occur. This also requires some continuous exchange of data between the devices to keep track of the state of the VPN's SA information. Multiple active VPN tunnels are also implied to be setup. In this situation, when a failure of one path occurs, an immediate switch of traffic to an alternate and operational tunnel can be accomplished. This is a benefit over stateless failover where the traffic is unprotected until the new tunnel is established. Since there are multiple VPNs already established, the traffic is protected if one tunnel goes down and it fails over to the other tunnel.

Through the use of active (primary) and backup (secondary) devices, stateful failover is accomplished. This is similar to HSRP but SA information is also being maintained. Upon failure of the primary path, the backup router automatically forwards the traffic and is transparent to both the users and the remote VPN peer.

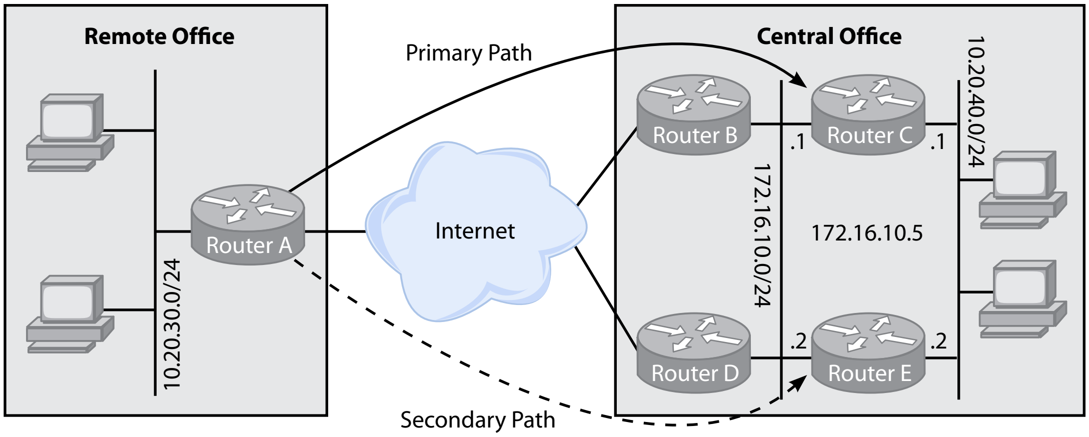
IPSec stateful failover utilizes two protocols for proper and continual operation. These are:

- **HSRP** – Both the inside and outside interfaces are monitored and if either goes down, the entire router is deemed down and ownership of the IKE and IPSec SA processes are passed over to the standby router. This makes the standby router the active HSRP router.
- **Stateful Switchover (SSO)** – This shares the IKE and IPSec SA information between the active and backup routers. Either router knows enough to be the active VPN router at any time.

Some limitations/restrictions exist when using IPSec stateful failover.

- Active and standby devices must be running the same Cisco IOS release.
- Active and standby devices must be connected via LAN ports, either directly or through a switch and WAN interfaces are not supported.
- The inside and outside interfaces must be connected via LAN ports.
- Only device-to-device failover is supported where intrachassis (card-to-card) failover is currently not supported.
- Only one device in a group can be active at any one time and load balancing is not supported.
- DPD and periodic DPD are supported but IKE keepalive messages are not.
- L2TP stateful failover is not supported.
- IPSec idle timers are not supported.

Since the IPSec stateful failover uses HSRP and SSO, both must be configured properly. The configuration is listed in Figure 25.



Router C:

```
crypto dynamic-map from-remote 10
  set transform-set trans1
  reverse-route

crypto map central-office 10 ipsec-isakmp dynamic from-remote

interface fastethernet 1/0
  ip address 172.16.10.1 255.255.255.0
  standby 1 ip 172.16.10.5
  standby 1 priority 150
  standby 1 preempt
  standby 1 name vpn-remote
  crypto map central-office redundancy vpn-remote stateful
```

```
redundancy inter-device
  scheme standby vpn-remote

ipc zone default
  association 1
  protocol sctp
    local-port 12321
  local-ip 10.20.40.1
  retransmit-timeout 300 10000
  path-retransmit 10
  assoc-retransmit 20
    remote-port 12321
  remote-ip 10.20.40.2
```

Figure 25

The configuration in Figure 25 is identical to Router C's configuration in Figure 24, but has the addition of **stateful** to the crypto map on the interface and the HSRP configuration is the same as before. This allows the use of SSO to perform stateful failover. To complete the stateful configuration, Router E would have a similar configuration to Router C.

The IOS commands to enable SSO are shown in the follow-on configuration box in Figure 25. In order to configure redundancy and enter inter-device configuration mode, issue the **redundancy inter-device** command. The only scheme supported currently is **standby** and the name of the standby must match the standby group name defined with the crypto map on the interface.

To configure the inter-device communication protocol (IPC) between the devices, the **ipc zone default** command initiates the communication link between active and standby routers. The subcommand **association** creates an association between the active and standby routers and uses the Stream Control Transmission Protocol (SCTP) as the transport protocol.

Local and remote SCTP ports and IP addresses are defined within SCTP. The *local-port* defined on this router must match the *remote-port* configured on the peer router and the *local-ip* and *remote-ip* addresses should point to physical interface IP addresses and not virtual IP addresses.

The definition of the number of SCTP retries before an attempt to create an SCTP session fails is set by the **path-retransmit** command. The **retransmit-timeout** command defines the maximum amount of time that SCTP waits before retransmitting data.

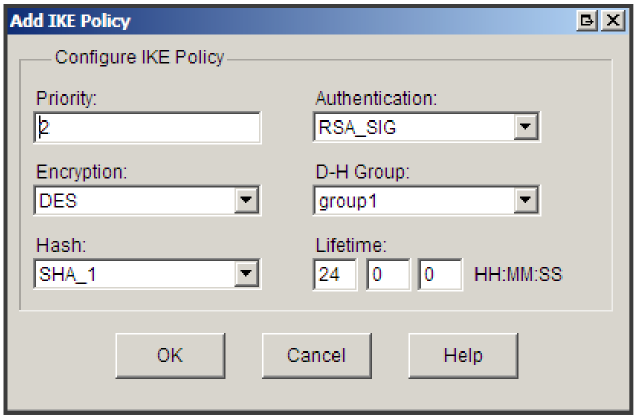
Configuring Cisco Easy VPN

There are two components that make up the Cisco Easy VPN solution, Server and Remote. The Cisco Easy VPN Server allows Cisco IOS Routers, Cisco PIX firewalls and Cisco VPN 3000 Concentrators to act as VPN headend devices in site-to-site or remote-access VPN models.

Easy VPN Server Configuration

The Easy VPN Server Configuration is done through SDM. This makes it easy since it's a point-and-click interface. Start SDM and select **Configure** on the top menu bar. Select **VPN** on the left side-bar, which is where you can configure Easy VPN Server and Remote. Select **Easy VPN Server** on the side menu which will give you some options. It will also tell you that AAA needs to be setup on the device if it isn't already. You have to have AAA enabled to proceed with the setup. Once AAA is configured, click **Launch Easy VPN Server Wizard** to start the wizard.

The first screen shows the steps needed to configure Easy VPN on the device. Click **Next** to proceed. This screen is where you select which interface to use for the VPN connection and whether to use pre-shared keys, digital certificates or both. Once you select the interface and type of authentication, click **Next** to continue. The next screen is where IKE proposals will be configured. There is a default proposal but you can add your own. By adding your own proposal, you can select stronger settings for your VPN connection. Figure 26 shows the screen to add your own proposal.

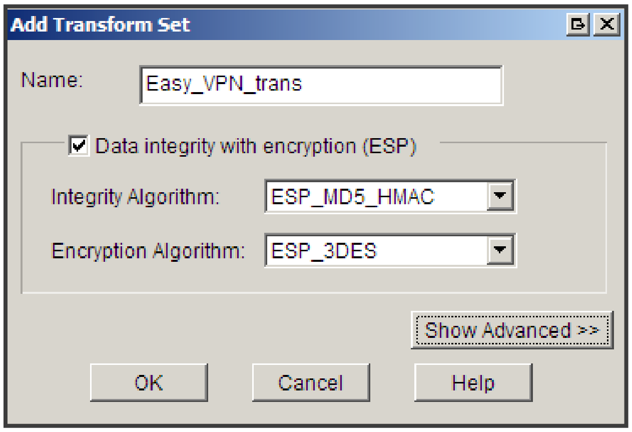


Priority: 2
Authentication: RSA_SIG
Encryption: DES
D-H Group: group1
Hash: SHA_1
Lifetime: 24 0 0 HH:MM:SS

Figure 26

The priority option is to set the proposal higher in the list so it's used before others. Authentication is to choose whether pre-shared keys or digital certificates are used. Encryption determines how strong the encryption method is, and you can select DES or 3DES. D-H Group is for the Diffie-Hellman Group to use; the options are 1, 2 and 5. Hash is for data integrity which is SHA1 or MD5. The lifetime is the security association (SA) lifetime. In Figure 26, the SA lifetime will expire after 24 hours and a new one will be created. Once all options are chosen, click **OK** to add it to the list. If you have other proposals in the list, you can select one and click **Edit** to change the options for that proposal. Once you have all proposals entered, click **Next** to continue to the transform-set page.

Like the IKE proposals page, you can select the default in the list or create your own. Figure 27 shows the options page for adding a transform-set.



Add Transform Set

Name: Easy_VPN_trans

☑ Data integrity with encryption (ESP)

Integrity Algorithm: ESP_MD5_HMAC

Encryption Algorithm: ESP_3DES

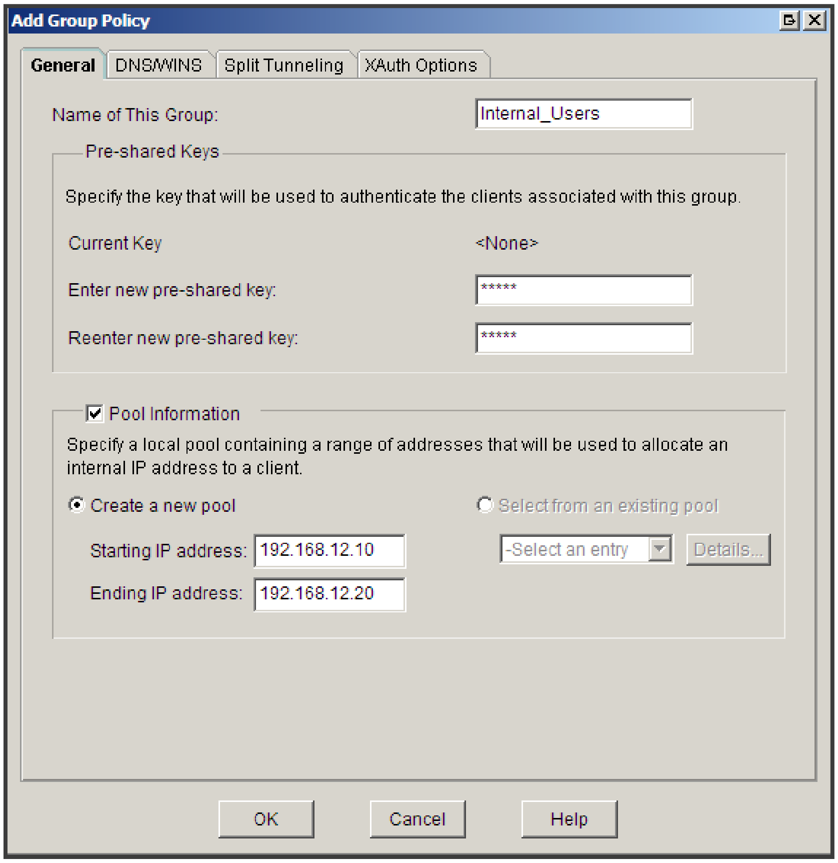
Figure 27

This section is a little easier to configure. You provide a name for the transform-set, select the Integrity Algorithm and Encryption Algorithm. Once done, click **OK** to add this transform-set to the list. Once added, the new transform-set will be selected and you can click **Next** to continue on to Group Authorization and Group Policy Lookup.

On this screen, you will choose whether it will be a local database, one on the router, using a RADIUS server, or using a RADIUS server and then a local database if the RADIUS server cannot be reached. If you select RADIUS then you will have the option to enter the information for the RADIUS server. Click **Next** to continue to the XAuth screen.

User Authentication, or XAuth, provides additional security by authenticating the user of a device after the device has undergone IKE authentication. The user credentials can either be on the device, a RADIUS server, a RADIUS server and then a local database if the RADIUS server cannot be reached, or an existing AAA method list can be selected with the server information. Click the **Add User Credentials** button to add other users to the list. Once everything is set, click **Next** to add Group Authorization and User Group Policies.

This screen allows you to add groups and their pertinent network settings. Figure 28 shows the screen options.



Name of This Group: Internal_Users

Pre-shared Keys

Specify the key that will be used to authenticate the clients associated with this group.

Current Key <None>

Enter new pre-shared key: *****

Reenter new pre-shared key: *****

☑ Pool Information

Specify a local pool containing a range of addresses that will be used to allocate an internal IP address to a client.

● Create a new pool ○ Select from an existing pool

Starting IP address: 192.168.12.10 -Select an entry Details...

Ending IP address: 192.168.12.20

Figure 28

A group name is specified along with pre-shared keys and a DHCP pool. You can enter DNS and WINS server addresses and setup split tunneling. Split tunneling allows users to traverse the VPN to access resources on the other network but keep their local connectivity for Internet access. Once everything is set, click **OK** to add the group to the list. Clicking **Next** will take you to the summary page so that you can review the settings. If any of the settings are incorrect, go back to that section and correct them. Click **Finish** to apply the Easy VPN configuration to the device.

Describe Network Security Strategies

A number of router services are considered security threats. In order to keep intruders out, it is best to minimize the services running on the router. It is a tedious process to disable all unnecessary services on all routers and is best left for the perimeter routers. The services are grouped into categories and cover the three subcategories for this portion of the test.

Unnecessary Services and Interfaces

Service	Description	Default	Disable
Router interfaces	Provide packet access in and out. By disabling the interface, you prevent it from becoming active if a cable is plugged into it.	Disabled (in a Cisco router with no user configuration)	(config-if)#**shutdown**
BOOTP server	Service permits the router to act as a BOOTP server for other network devices.	Enabled	(config)#**no ip bootp server**
Cisco Discovery Protocol (CDP)	This periodically advertises information between Cisco devices which could be helpful to an attacker.	Enabled (globally and interface)	(config)#**no cdp run** (config-if)#**no cdp enable**
Configuration auto-loading	Service permits a router to automatically load a configuration file from a network server upon boot.	Disabled	(config)#**no service config**
FTP server	Service permits the router to act as an FTP server for specific files in flash memory.	Disabled	(config)#**no ftp-server enable**
TFTP server	Service permits the router to act as a TFTP server for specific files in flash memory.	Disabled	(config)#**no tftp-server** *file-sys: image-name*
NTP service	Service both receives time-of-day clock from NT server and allows the router to act as an NTP server to NTP clients.	Disabled	(config)#**no ntp server** *ip-address*
Packet assembler/ disassembler (PAD) service	Service allows access to X.25 PAD commands in an X.25 network.	Enabled	(config)#**no service pad**
TCP and UDP minor services	Services execute small servers in the router, typically used for diagnostics.	Enabled (before 11.3) Disabled (11.3 and greater)	(config)#**no service tcp-small-servers** (config)#**no service udp-small-servers**
Maintenance Operation Protocol (MOP) service	Service is a Digital Equipment Corporation (DEC) maintenance protocol.	Enabled (most Ethernet interfaces)	(config-if)#**no mop enabled**

Common Management Services

Service	Description	Default	Disable
Simple Network Management Protocol (SNMP)	Service permits the router to respond to queries and configuration requests.	Enabled	(config)#**no snmp-server enable**
HTTP Configuration and Monitoring	Service allows the router to be monitored and configured from a web browser. SDM uses HTTPS.	Device dependant	(config)#**no ip http server** (config)#**no ip http secure-server**
Domain Name Service (DNS)	Cisco routers use 255.255.255.255 as the default address to reach a DNS server for name resolution.	Enabled (client service)	(config)#**no ip domain-lookup**

Path Integrity Mechanisms

Service	Description	Default	Disable
ICMP Redirects	Service causes the router to send an ICMP redirect message when a packet is forwarded out the interface it arrived on.	Enabled	(config)#**no ip icmp redirect** (config-if)#**no ip redirects**
IP Source Routing	Service allows the sender to control the route that a packet travels through a network.	Enabled	(config)#**no ip source-route**

Probes and Scans

Service	Description	Default	Disable
Finger service	The finger protocol (port 79) retrieves a list of users from a network device, which includes the line number, connection name, idle time and terminal location.	Enabled	(config)#**no service finger**
ICMP unreachable notification	Service notifies a sender of invalid destination IP subnets or specific addresses.	Enabled	(config)#**no ip unreachables**
ICMP mask reply	Service sends the IP subnet mask when it is requested.	Disabled	(config)#**no ip mask-reply**
IP directed broadcasts	A directed broadcast can be used to probe or deny service to (via a DoS attack) an entire subnet.	Enabled (Cisco IOS Software releases prior to 12.0) Disabled (Cisco IOS Software Release 12.0 and later)	(config-if)#**no ip directed-broadcast**

Terminal Access Security

Service	Description	Default	Disable/Enable
IP identification service	The identification protocol (RFC 1413) reports the identity of the TCP connection initiator.	Enabled	(config)#**no ip identd**
TCP keepalives	TCP keepalives help clean up TCP connections when a remote host has stopped processing TCP packets.	Disabled	To enable (config)#**service tcp-keepalives-in** (config)#**service tcp-keepalives-out**

Gratuitous and Proxy ARP

Service	Description	Default	Disable
Gratuitous ARP	Service is the primary means used in ARP poisoning attacks.	Enabled	(config)#**no ip arp gratuitous**
Proxy ARP	Service permits the router to resolve Layer 2 addresses.	Enabled	(config)#**no ip arp proxy**

Implement Cisco Device Hardening

Using AutoSecure to Secure a Router

Since CLI commands are needed to manually disable services, some routers may not be as secure as they should be. To help alleviate this issue, Cisco introduced the AutoSecure feature. AutoSecure helps administrators secure the devices by automatically performing a variety of functions. The AutoSecure feature is available with IOS release 12.3 or higher. There are two modes for AutoSecure, automatic and interactive. Using automatic mode, default settings are applied to all security settings. Interactive mode allows the user to select options and features individually. The following functions are performed with AutoSecure:

- **Management plane services and functions** – Finger, PAD, UDP and TCP small servers, password encryption, TCP keepalives, CDP, BOOTP, HTTP, source routing, gratuitous ARP, proxy ARP, ICMP redirects, ICMP mask replies, directed broadcast, MOP and banner.
- **Forwarding plane services and functions** – CEF and ACLs which affect every packet flowing through the router.
- **Firewall services and functions** – Includes IOS firewall inspection for common protocols which permits deep packet inspection.
- **Logging functions** – Event logging and password security to keep track of events.
- **NTP** – NTP is securely configured to prevent abuse of the NTP information.
- **SSH access** – Encrypted SSH access is preferred to clear-text Telnet to prevent packet sniffers from capturing telnet session data.
- **TCP intercept services** – Prevention of TCP SYN-flooding attacks. Basically, preventing DoS attacks.

To enable AutoSecure, issue the following command from privileged mode, not configuration mode:

```
Router# auto secure [management | forwarding] [no-interact | full] [login | ntp | ssh | firewall |
 tcp-intercept]
```

The default option for this command is **full** which means the user is prompted for input to all security features interactively. Automatic mode is initiated by issuing **no-interact** which applies the default configurations to all security parameters. You can implement any option by issuing that command. In order to secure management, you would issue **Router# auto secure management** and only one option is allowed at a time. You would have to issue each option on a separate line. Using the **auto secure full** command would perform the following steps in sequence:

- **Identify the outside interface(s)** – Selects the Internet-facing interfaces.
- **Secure the management plane** – Enable and/or disable services and functions.
- **Create a security banner** – Configures a message that is displayed when the router is accessed.
- **Configure passwords, AAA and SSH** – Configures secure modes/features to access the router. This includes minimum password length, login failure tolerance, AAA and enable SSH instead of telnet.
- **Secure the interfaces** – Disables various features such as no ip redirects, no ip proxy-arp, no ip unreachables, no ip directed-boradcast, no ip mask-reply and no mop enabled. These are applied to Ethernet interfaces.
- **Secure the forwarding plane** – Enables CEF, uRFP (if possible) and CBAC, which is the router firewall feature.

The two ways to mitigate the failure of the AutoSecure process are:

- Manually save the running configuration to either NVRAM, flash or a network server prior to starting the AutoSecure process. If AutoSecure only installs a partial configuration, you can go back to the untouched copy of the configuration file.
- Part of the AutoSecure process on a device running IOS release 12.3(8)T is to create a copy of the running configuration file for you. You can restore the configuration by issuing **configure replace flash:pre_autosec.cfg** which is a snapshot of the running configuration file.

Using SDM to Secure a Router

There are two separate wizards which help secure the router, Security Audit or One-step Lockdown. You can choose either by clicking **Configure** on the top menu bar and choosing **Security Audit** in the Tasks bar to the left.

The Security Audit option performs the following functions:

- The running configuration is checked against a list of predefined security configuration settings.
- Lists identified problems and provides recommendations for fixing them.
- Allows the user to choose which identified problem(s) to fix. It then displays the appropriate user interface to fix them.
- Applies the user-chosen security configuration to the router.

The One-Step Lockdown Wizard does just what it says. You click One-step lockdown on the Security Audit configuration page and you are presented with a warning. It lets you know it will lockdown the router and what to do to undo some of the settings. Once you click **Yes**, the process starts and it does not provide any user-configurable options.

Using AAA to Scale Access Control

AAA stands for authentication, authorization and accounting. Authentication is "Who are you?" This determines whether the user is who they say they are by use of a username and password. Authorization is "What is the user allowed to do?" The username you use depends on what access you have to the device. Accounting is "What have the users been doing on the network?" This can include length of time a VPN was used, how many times it was used by a specific user or how many users are using a given network resource. Only after authentication is established are authorization and accounting enabled.

The two services which provide AAA services for networks is TACACS+ and RADIUS. RADIUS relies on UDP and TACACS+ relies on TCP. This makes TACACS+ a better solution since it uses a connection-oriented session instead of a connectionless session. TACACS+ allows for the encryption of the entire body of the packet, whereas RADIUS encrypts only the password within the access-request packet. Since RADIUS sends the username in cleartext, this would be a security risk.

TACACS+ separates authentication and authorization. It is routine within TACACS+ to use a Kerberos server for authentication and a TACACS+ server for authorization. RADIUS combines authentication and authorization into a single request, which makes designing a system to separate authentication and authorization to different servers difficult. A wide array of protocols is supported by TACACS+, where RADIUS does not support AppleTalk Remote Access protocol, NetBIOS Frames Protocol Control protocol, Novell Asynchronous Services Interface (NASI) or X.25 PAD connection.

Configuring AAA Using CLI

RADIUS configuration:

```
aaa new-model
radius-server host 10.20.30.9
radius-server key TheRADIUSServerKey
username root password TheSecretPassword
aaa authentication ppp mydiallist radius local
aaa authorization network radius local
aaa accounting network mynetwork start-stop group radius
```

TACACS+ Configuration

```
aaa new-model
tacacs-server host 10.20.30.8
tacacs-server key TheTacacsServerKey
username root password TheSecretPassword
aaa authentication ppp mydiallist tacacs+ local
aaa authorization commands 15 tacacs+ if-authenticated none
aaa accounting network start-stop tacacs+
```

AAA Related Commands

The command **aaa new-model** enables AAA on the router. To disable AAA, issue **no aaa new-model**.

radius-server host *parameters*

Parameter	Description
hostname	The name of the RADIUS server
ip-address	IP address of the RADIUS server
auth-port	UDP destination port for authentication requests
port-number	Port number for authentication requests: 0 = no host used; default = port 1645
acct-port	UDP destination port for accounting requests
port-number	Port number for accounting: 0 = no host used; default = port 1646
timeout	Number of seconds the router waits for a response from the RADIUS server before sending the request
seconds	Timeout value
retransmit	Number of times a RADIUS request is retransmitted
retries	Retransmit value
key	An authentication and encryption key will be used by the router and the RADIUS server.
string	The key used for authentication and encryption
alias	Up to eight aliases to be used for a given RADIUS server

tacacs-server host *parameters*

Option	**Description**
hostname	Name of the RADIUS server
ip-address	IP address of the RADIUS server
key	The authentication and encryption key used by the router and the TACACS+ server
string	Key used for authentication and encryption
nat	The NAT address of the client that is sent to the TACACS+ server
port	TACACS+ server port number (default = 49)
integer	Port number of the TACACS+ server
single-connection	Maintains a single open connection between the router and the TACACS+ server
timeout	Specifies a timeout value
integer	Value in seconds for TCP timeout

radius-server key and **tacacs-server key**

Option	**Description**
0 *string*	Unencrypted key is *string*
7 *string*	Hidden key is *string*
string	Unencrypted key is *string* and is the same as the 0 *string*

username root password command is not AAA specific and specifies a username and password combo.

aaa authentication ppp specifies the AAA authentication methods used on serial interfaces running point-to-point protocol.

Option	**Description**
default	When a user logs in, uses the authentication methods following the parameter as the default list
list-name	String used to name the list of methods when the user logs in
methods1 [method2]	At least one of the following methods is used: if-needed – do not authenticate if the user is already authenticated krb5 – use Kerberos 5 for authentication local – use the local database none – no authentication radius – use RADIUS authentication tacacs+ - use TACACS+ authentication

aaa authorization *parameters*

Option	**Description**
network	Runs authorization for all network-related service requests
exec	Runs authorization to determine if the user is authorized to run an EXEC shell
commands	Runs authorization for all commands at the specified level
level	Command level that should be authorized; level may be from 0 through 15
reverse-access	Runs authorization for reverse access connections (reverse Telnet)
default	The authentication methods following the parameter as the default list when a user logs in
list-name	String used to name the list of methods used when the user logs in
method1 [method2]	At least one of the following methods is used: if-needed – do not authenticate if the user is already authenticated krb5 – use Kerberos 5 for authentication local – use the local database none – no authentication radius – use RADIUS authentication tacacs+ - use TACACS+ authentication

aaa accounting *parameter*

Option	Description
auth-proxy	Accounting for all authenticated proxy events
system	Accounting for all system-level events not associated with users (reboots and such)
network	Accounting for all network-related requests
exec	Accounting for all EXEC shell sessions
connection	Accounting for all outbound connections from the network access server
commands *level*	Accounting for all commands at the specified level
default	Uses the listed accounting methods that follow
list-name	String used to name the list; valid options are group radius – list of RADIUS servers group tacacs – list of TACACS+ servers group *group-name* – a subset of RADIUS and TACACS+ servers
vrf *vrf-name*	Specifies a VRF configuration
start-stop	Sends a "start" notice at the beginning of a process and a "stop" notice at the termination of the process
stop-only	Sends a "stop" notice at the end of a process
broadcast	Enables sending accounting records to multiple AAA servers
group *group-name*	String used to name the list; valid options are group radius – list of RADIUS servers group tacacs – list of TACACS+ servers group *group-name* – a subset of RADIUS and TACACS+ servers

Using Debugging for AAA

To verify and troubleshoot AAA, there are five commands that can be used. Table 22 lists these commands.

Command	**Description**
debug aaa authentication	Displays information on authentication events
debug aaa authorization	Displays information on authorization events
debug aaa accounting	Displays information on accounting events
debug radius	Displays information associated with RADIUS
debug tacacs	Displays information associated with TACACS+

Table 22

Threat and Attack Mitigation Using ACLs

Locking down a router based on Access Control Lists (ACLs) can be either simple or complex. ACLs can be setup to block/filter by IP address, port or any other criterion within the assigned access list. An access list has adds a deny statement at the end but, unless you implicitly add a deny statement, it won't show up in any logs as blocking ingress into the router/network. Below is a simple access list allowing traffic to a specific internal IP address:

```
Router(config)#access-list 100 permit tcp any host 10.10.20.4
Router(config)#access-list 100 deny ip any any log
Router(config)#interface serial 1/1
Router(config-if)#ip access-group 100 in
Router(config-if)#end
```

Implement Cisco IOS Firewall

Cisco IOS Firewall Feature Set

The IOS Firewall feature set has the following three main features:

- Cisco IOS Firewall
- Authentication Proxy
- Intrusion Prevention System (IPS)

Cisco IOS Firewall

This is a stateful packet filter and has the following features:

- Permits or denies specified TCP and UDP traffic
- Maintains a state table
- Modifies ACLs dynamically
- Protects against DoS attacks
- Inspects packets passing through the interface

Authentication Proxy

This provides authentication and authorization on a per-user basis through either RADIUS or TACACS+ for the following protocols:

- HTTP
- HTTPS
- FTP
- Telnet

Cisco IOS IPS

This is an intrusion detection and response system that identifies and responds to over 700 forms of attack. Once an attack is identified, it initiates one or more of the actions in Table 23.

Action	Description
Drop	Drops the packet
Block	Blocks the sending IP address for a specified period of time
Reset	Terminates a TCP session by sending a TCP reset
Alarm	Sends an alarm to the syslog server or SDM

Table 23

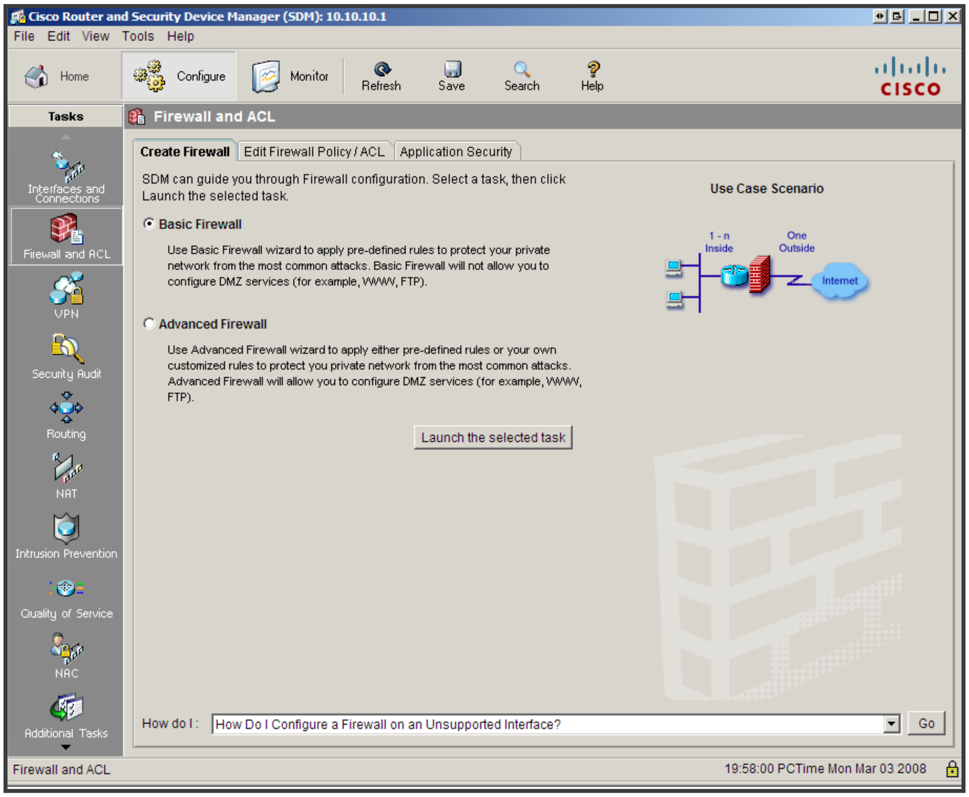
The capabilities of the Cisco IOS Firewall are listed in Table 24.

Capability	Benefit
Layered defense	A breach in one area does not compromise all of the network.
Packet filtering	May block specific types of packets.
ALG	The end user never connects directly to the resource.
Stateful packet filtering	Tracks the state of a connection and drops those packets that are not authorized.
Cisco IOS Firewall	Filters packets based on session and application.
Cisco IOS Authentication Proxy	Enables use of RADIUS or TACACS+.
Cisco IOS IPS	Identifies over 700 common attacks and refutes them.
Logging	Allows real-time logging of any or all events.

Table 24

Configure IOS Firewall Using SDM

Using SDM to configure the IOS firewall is fairly straight forward. As shown in Figure 29, you have two options for the firewall, basic and advanced.



SDM can guide you through Firewall configuration. Select a task, then click Launch the selected task.

● Basic Firewall

Use Basic Firewall wizard to apply pre-defined rules to protect your private network from the most common attacks. Basic Firewall will not allow you to configure DMZ services (for example, WWW, FTP).

○ Advanced Firewall

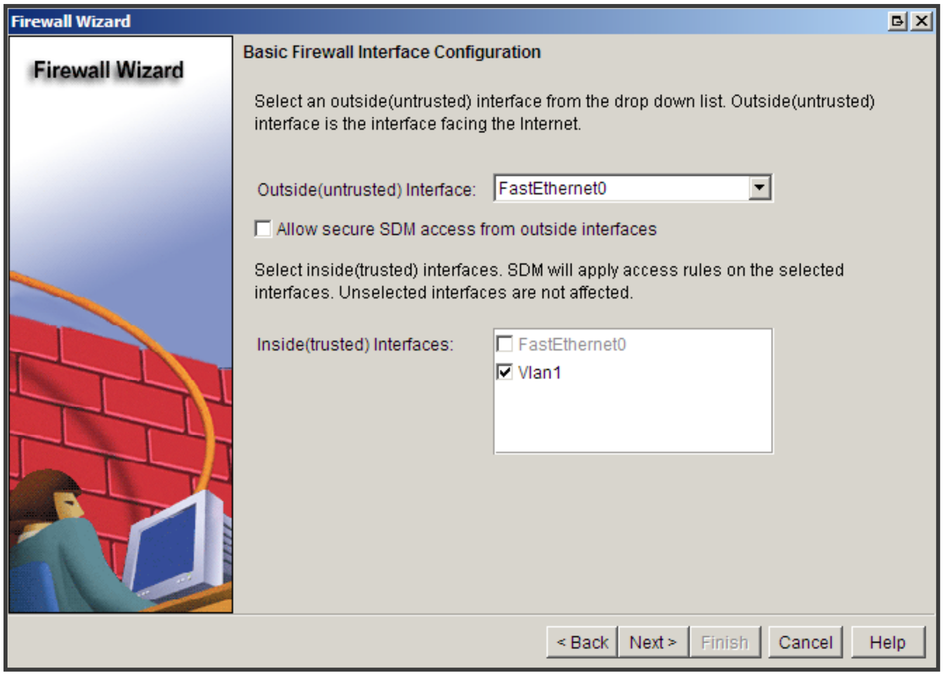
Use Advanced Firewall wizard to apply either pre-defined rules or your own customized rules to protect you private network from the most common attacks. Advanced Firewall will allow you to configure DMZ services (for example, WWW, FTP).

How do I : How Do I Configure a Firewall on an Unsupported Interface?

Firewall and ACL 19:58:00 PCTime Mon Mar 03 2008

Figure 29

Select Basic Firewall and click **Launch the selected task** to continue. You are presented with a screen that lists which tasks will take place. It will apply default access rules to the inside (trusted) and outside (untrusted) interfaces, apply default inspection rule to outside interface, and enable IP unicast reverse-path forwarding to the outside interface. Clicking **Next** takes you to the Basic Firewall Interface configuration screen. Here you select which is the outside interface and the inside interface. There is a check-box to allow secure SDM access from the outside interface as shown in Figure 30.



Basic Firewall Interface Configuration

Select an outside(untrusted) interface from the drop down list. Outside(untrusted) interface is the interface facing the Internet.

Outside(untrusted) Interface: FastEthernet0

□ Allow secure SDM access from outside interfaces

Select inside(trusted) interfaces. SDM will apply access rules on the selected interfaces. Unselected interfaces are not affected.

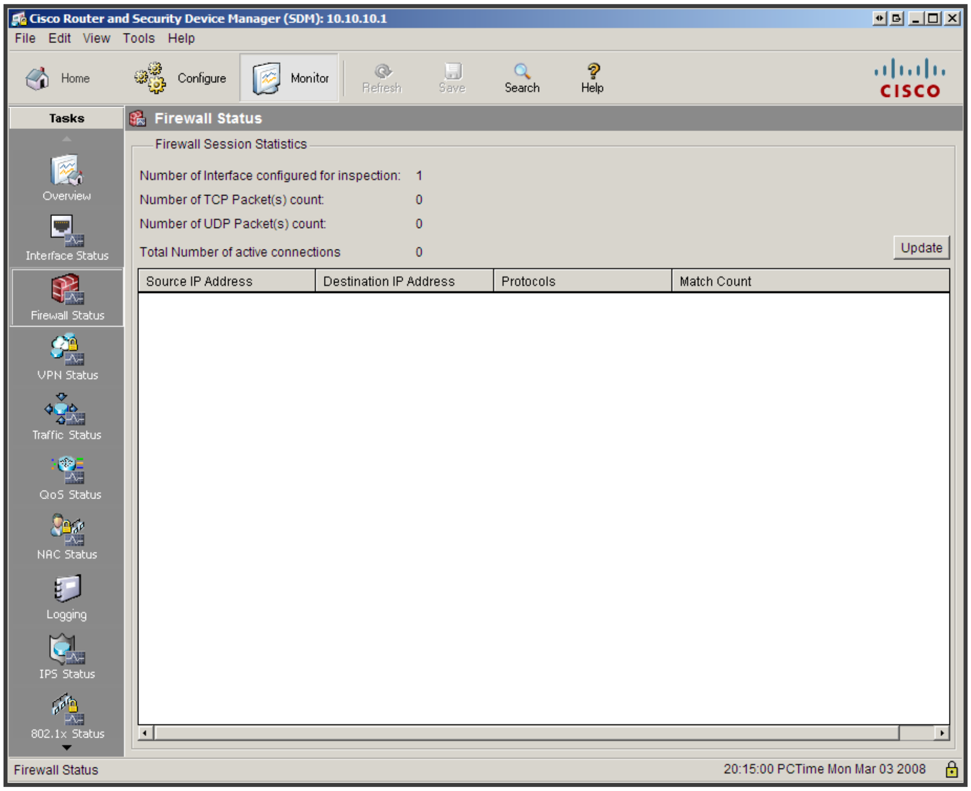
Inside(trusted) Interfaces:
□ FastEthernet0
☑ Vlan1

Figure 30

Once the interfaces are selected, and depending on whether or not you want to allow secure SDM access from the outside interface, click **Next** to continue. The Firewall Configuration Summary is presented and lists which options are going to be applied to the router. Click **Finish** to apply the configuration to the router. This will deny spoofing traffic, traffic sourced from broadcast and local loopback addresses, and permit all other traffic to the inside interface. The configuration will turn on unicast path forwarding check and permit IPSec tunnel traffic, GRE tunnel traffic, ICMP traffic, NTP traffic, and will deny spoofing traffic, traffic sourced from broadcast, local loopback and private address, and denies all other traffic.

Verify IOS Firewall Configuration

Verification can take place one of two ways, command line and SDM. Figure 31 shows the SDM screen to monitor the firewall.



Firewall Status

Firewall Session Statistics

Number of Interface configured for inspection: 1
Number of TCP Packet(s) count: 0
Number of UDP Packet(s) count: 0
Total Number of active connections 0

Source IP Address	Destination IP Address	Protocols	Match Count

Figure 31

This screen will show number of interfaces configured for inspection, number of TCP packet(s) count, number of UDP packet(s) count and total number of active connections. The box below this will show the source and destination IPs, along with the protocols being used and any matches to the firewall rules.

To verify the configuration via CLI, the **show ip inspect** command is issued.

show ip inspect *command options*

Parameter	**Description**
name *inspection-name*	Displays the configured inspection with the defined inspection name
config	Displays the entire IP inspection configuration
interface	Displays the configurations used within the interface mode
session	Displays sessions that are currently being tracked
detail	Displays additional details about current sessions
statistics	Displays statistical information
all	Displays all information

The debug command can also be issued to troubleshoot the configuration. Below are the command options for the **debug ip inspect** command.

debug ip inspect *commands*

Command	**Description**
debug ip inspect function-trace	Debugs the functions used by ip inspect
debug ip inspect object-creation	Debugs the creation of objects used by ip inspect
debug ip inspect object-deletion	Debugs the deletion of objects used by ip inspect
debug ip inspect events	Debugs events within ip inspect
debug ip inspect timers	Debugs timers used in ip inspect
debug ip inspect detail	Provides detailed debugging of ip inspect

Describe and Configure Cisco IOS IPS

Two types of intrusion systems are typically deployed in networks today: intrusion detection systems (IDS) and intrusion prevention systems (IPS). Each consists of either hardware or software which detects network anomalies. How each system reacts to anomalies determines its role.

An IDS device sits off to the side and not directly in the traffic flow. The traffic is copied to the IDS device for inspection. If the device determines that packets are not of good intentions, it sends an alert to a management station for further action. It can also actively configure network devices, such as routers and firewalls, to clock or quarantine the bad packet flows. It does not block packets itself since it does not sit in the data path. Hence, by the time it detects anomalies, the first few packets have entered the network.

An IPS device sits directly in the path of the packet flow. All packets must flow through the device to get to their destination. Since it is in the path of the data flow, it can detect anomalies and both block the packets and notify a management station for further action. There is also no need to configure any other devices on the network to block the bad packets.

IPS is useful for detecting viruses, worms, malicious applications and vulnerability exploits, none of which should be permitted into the network and are defined below.

- **Virus** – A type of malicious code that tries to propagate itself across a network by attaching itself to other programs and then executes a particular unwanted function.
- **Worm** – A type of malicious code that executes arbitrary code and installs copies of itself in the memory of the infected computer. It then spreads to and infects other hosts. Unlike a virus which cannot propagate across the network by itself, a worm can spread automatically.
- **Trojan horse** – This is a general term that refers to a program which appears desirable but is actually bad. This can be in the form of a game download, document, spreadsheet, etc. The malicious contents can contain a virus or worm.
- **Vulnerability exploit** – An attack that specifically targets a known device vulnerability.

IDS and IPS can be used together to make the network security tighter. IDS and IPS systems can be categorized by the following:

- **Signature-based** – These systems match for a specific byte pattern or content in a packet. Pattern matching is typically combined with particular IP address, protocol and/or port combination.
- **Policy-based** – These systems use algorithms to examine strings of packets to determine patterns and behavior. This approach might detect a ping sweep.
- **Anomaly-based** – These systems look for behavior which deviates from the "norm". This is to imply that some definition of "normal" is dynamically learned by or preprogrammed into the system before it can detect anything abnormal.

IDS and IPS Signatures

A signature is a pattern of data or traffic that should cause a reaction when it passes through the IDS or IPS. This reaction can be to either send some type of alert or actively block the bad traffic.

The IDS and IPS use microengines to match signatures against packets and packet flow. There are four categories of IDS and IPS signatures:

- **Exploit** – This typically identifies malicious traffic by matching a traffic pattern. Since each exploit has a unique signature, each attack requires a signature for detection.
- **Connection** – This signature is aware of valid network connections and protocols. Any actions that occur beyond the normal circumstances are considered suspect, since the behavior of accepted connections and protocols is known in advance.
- **String** – This signature typically uses regular expressions to match patterns. An exploit signature usually matches a single exploit, whereas a regular expression can be used to match many conditions.
- **DoS** – This signature examines behavior typical of a DoS attack. Since there are many forms of DoS attacks, there are a variety of signatures used. If there is a behavioral change in a DoS attack, then an update to the DoS signature engine is required.

There are 100 signatures embedded in Cisco IOS Software, with a total of 132 including all of the subsignatures. Additional signatures can be downloaded from Cisco.com and individual signatures within an SDF can be enabled or disabled.

Signature Reaction

When a signature is matched, an IDS and IPS device reacts immediately. Alert messages can be sent with either syslog or the Security Device Event Exchange (SDEE) protocol.

Signature reactions include the following:

- **Send an alarm to a syslog or centralized management server** – Normally, an alarm notification is not the only action.
- **Drop the packet** – This action should not affect a legitimate user if the source IP address is spoofed, as is the case in DoS attacks.
- **Reset the connection** – This works on connection-oriented protocols only, such as TCP. This will have no effect on UDP packet flows.
- **Block network traffic from the source IP address for a specified amount of time** – This imposes a penalty on the attacking traffic and permits time for attack analysis to occur. This should only be done if IP addresses are spoofed or else legitimate traffic is likely to be affected.
- **Block network traffic on the connection for a specified amount of time** – This, like the previous item, imposes a penalty on the attacking traffic. Due to the two-way communications needed for such traffic, connection-oriented attacks typically do not employ IP spoofing.

Configure Cisco IOS IPS using SDM

Using SDM to configure IPS, like other services through SDM, is straightforward. From the Configure screen, select the **Intrusion Prevention** button in the Tasks bar on the left side of the window. This will give you the two options below:

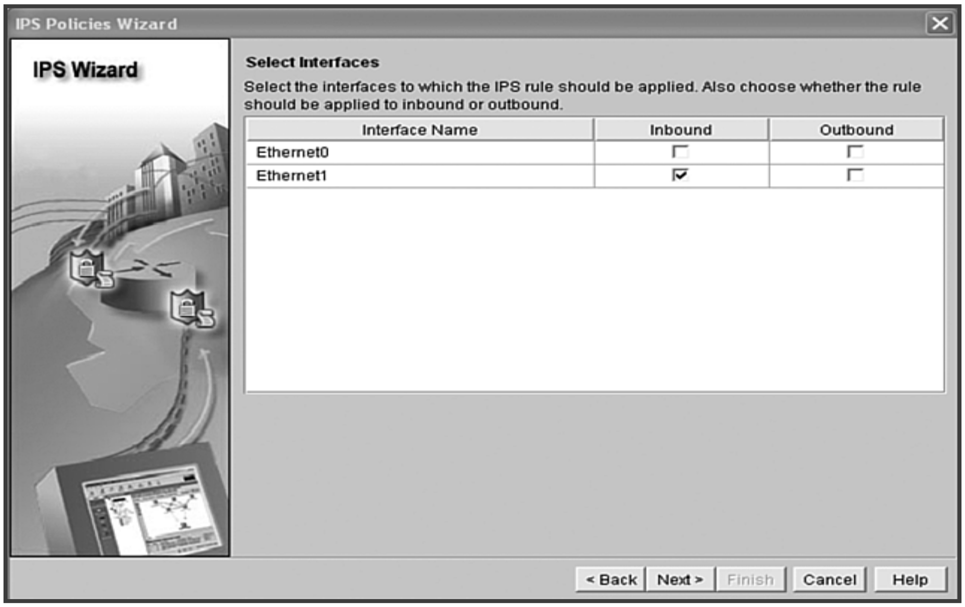
- **Create IPS** – Offers the opportunity to launch the IPS Rule Wizard to create new IPS rules
- **Edit IPS** – Allows access to all existing IPS policies, signatures and interface configurations

To create a new rule, click the **Launch IPS Rule Wizard** button on the Create IPS tab. A welcome screen is provided and lists the steps to be taken:

- Select the interface to apply the IPS rule to.
- Select the traffic flow direction that should be inspected by the IPS rules.
- Specify the location of the SDF to be used by the router.

Click **Next** to continue on to the wizard.

The first thing that needs to be done is to select the interface to inspect. This screen shows only the interfaces that have not been configured for inspection already. If you have not configured any interfaces for inspection, then all interfaces should be displayed. Figure 32 shows the interface screen.



Select Interfaces

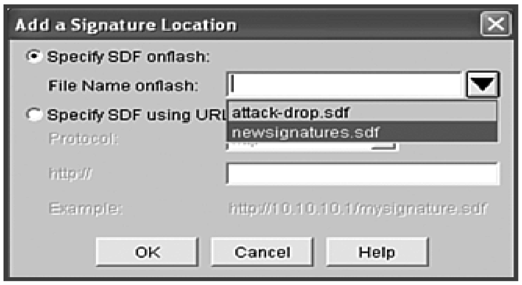
Select the interfaces to which the IPS rule should be applied. Also choose whether the rule should be applied to inbound or outbound.

Interface Name	Inbound	Outbound
Ethernet0	☐	☐
Ethernet1	☑	☐

Figure 32

Even though both Inbound and Outbound options are listed, it is best only to check the Inbound check box when IPS rules are applied. This will trigger the IPS as packets arrive and does not give them access to the router before being inspected. You will need to know which interface is attached to which segment, since only the interface name is listed and not its role.

Click **Next** to continue to the SDF Locations screen, which is where you select the signatures to use. If you want to add signatures to the default, click the **Add** button on the right of the window. Figure 33 shows the add signature window.



Add a Signature Location

● Specify SDF onflash:

File Name onflash:

attack-drop.sdf
newsignatures.sdf

○ Specify SDF using URL

Protocol:

http://

Example: http://10.10.10.1/mysignature.sdf

Figure 33

Click the **Specify SDF onflash** radio button and click the drop-down arrow to see the SDFs in flash. Click the desired SDF in the drop-down menu to enter it in the File Name onflash field. Now, click **OK** to add the specified file to the SDF locations. You can add multiple SDFs by selecting the add button for each SDF you wish to add.

The IPS will use the SDF that was just added and use the built-in signatures if the added SDFs are unavailable. To enable this, make sure the check-box is marked for the **Use Built-in Signatures (as backup)** option.

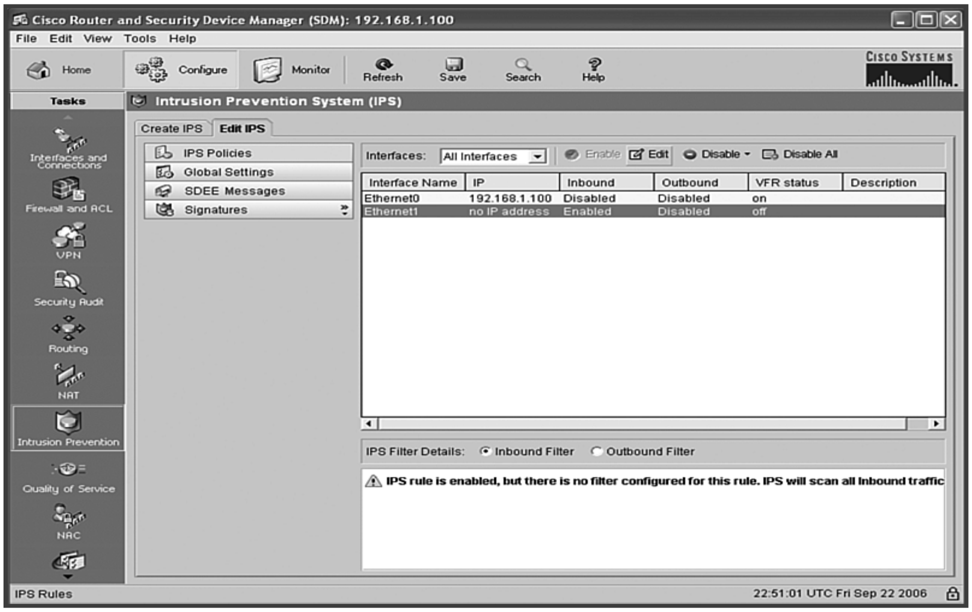
When you are finished adding additional SDFs, click the **Next** button to go to the summary screen. The summary screen will let you know which interface will be inspected and which signature file will be used. If there is an error, you can go back and correct it.

Clicking the **Finish** button will complete the creation of a new SDF and then push the configuration out to the router. When the configuration is pushed to the router and compiles the new signatures into the Cisco IOS IPS, a Signature Compilation Status screen is displayed. This will let you know which services will be inspected and the number of signatures for each. Click **Close** when done and you will be returned to the IPS Configuration window.

Edit IPS

If you click on the Edit IPS tab, you will be given four choices, which are shown in figure 34:

- **IPS Policies** – Allow you to enable and/or disable the IPS on any interface in the router, set the direction of the IPS, and add an access list to the IPS interface configuration so that only certain packets are inspected.
- **Global Settings** – Shows a summary of current IPS settings and allows you to add SDFs to, and delete SDFs from, the IPS.
- **SDEE Messages** – Shows the SDEE events.
- **Signatures** – Displays all signatures, by category, which are currently loaded. Here you can add, delete, enable, disable and edit individual signatures.



Interfaces: All Interfaces

Interface Name	IP	Inbound	Outbound	VFR status	Description
Ethernet0	192.168.1.100	Disabled	Disabled	on	
Ethernet1	no IP address	Enabled	Disabled	off	

IPS Filter Details: ● Inbound Filter ○ Outbound Filter

⚠ **IPS rule is enabled, but there is no filter configured for this rule. IPS will scan all Inbound traffic**

22:51:01 UTC Fri Sep 22 2006

Figure 34

Once you complete the Create IPS tab, the IPS is operational, so there is no need to apply the configuration to make it active after making changes. All operations performed from the Edit IPS tab are applied to the working configuration.