CHAPTER 37

More About....

These topics provide more information about subjects that Cisco SDM online help discusses.

IP Addresses and Subnet Masks

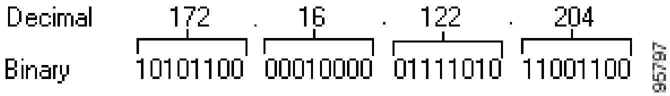
This topic provides background information about IP addresses and subnet masks, and shows you how to use this information when entering addresses and masks in Cisco SDM.

IP version 4 addresses are 32 bits, or 4 bytes, in length. This address "space" is used to designate the following:

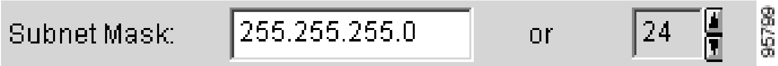
- Network number
- Optional subnetwork number
- A host number

Note Cisco SDM does not support IP version 6.

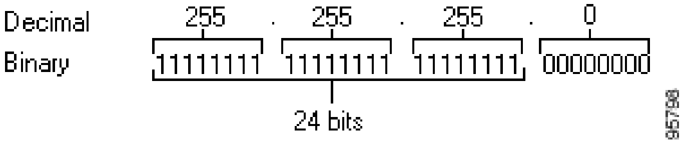
Cisco SDM requires you to enter IP addresses in dotted-decimal format. This format makes addresses easier for people to read and manipulate, by grouping the 32 bits into 4 octets which are displayed in decimal, separated by periods or "dots," for example, 172.16.122.204. The decimal address 172.16.122.204 represents the binary IP address shown in the following figure.



The subnet mask is used to specify how many of the 32 bits are used for the network number and, if subnetting is used, the subnet number. It is a binary mask with a 1 bit in every position used by the network and subnet numbers. Like the IP address, it is a 32-bit value, expressed in decimal format. The following figure shows a subnet mask entered in Cisco SDM. Cisco SDM shows the subnet mask and the equivalent number of bits in the mask.

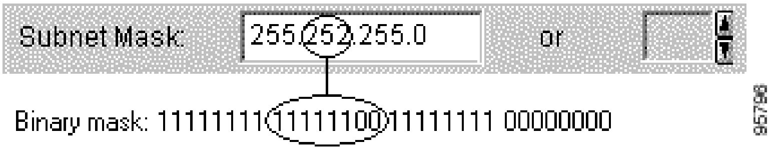

Subnet Mask: 255.255.255.0 or 24

These values entered Cisco SDM represent the binary mask shown in the following figure:



This subnet mask specifies that the first 24 bits of the IP address represent the network number and subnet mask, and that the last 8 bits represent the host number within that network and subnet. You can enter the mask in the dotted decimal format shown in the Subnet Mask field, or you can select the number of bits in the bits field. When you enter or select a value in one field, Cisco SDM automatically adjusts the other.

Cisco SDM displays a warning window if you enter a decimal mask that results in binary zeros (0s) in the network/subnet area of the mask. The following subnet mask field contains a decimal value that would result in binary zeros in the network/subnet number portion of the mask. Note that the bits field on the right is empty, indicating that an invalid value has been entered in the Subnet Mask field.



When a network address is displayed in Cisco SDM windows, the IP address and subnet mask for it may be shown in network address/subnet bits format, as in the following example:

```
172.28.33.0/24
```

The network address in this example is 172.28.33.0. The number 24 indicates the number of subnet bits used. You can think of it as shorthand for the corresponding subnet mask of 255.255.255.0.

Addresses used on the public Internet must be completely unique for the period of time they are being used. On private networks, addresses may be unique only to the private network or subnetwork.

Addresses may also be translated by using schemes such as NAT and PAT, and they may be temporarily assigned using DHCP. You can use Cisco SDM to configure NAT, PAT and DHCP.

Host and Network Fields

This topic explains how to supply host or network information in windows that allow you to specify a network or host address, or a host name.

Specify the network or the host.

Type

One of the following:

- **A Network**—If you select this, provide a network address in the IP address field. Note that the wildcard mask enables you to enter a network number that may specify multiple subnets.
- **A Host Name or IP Address**—If you select this, provide a host IP address or host name in the next field.
- **Any IP address**—The action you specified is to apply to any host or network.

IP Address/Wildcard Mask

Enter a network address, and then the wildcard mask to specify how much of the network address must match exactly.

For example, if you entered a network address of 10.25.29.0 and a wildcard mask of 0.0.0.255, any java applet with a source address containing 10.25.29 would be filtered. If the wildcard mask were 0.0.255.255, any java applet with a source address containing 10.25 would be filtered.

Host Name/IP

This field appears if you selected **A Host Name or IP Address** as Type. If you enter a host name, ensure that there is a DNS server on the network capable of resolving the host name to an IP address.

Available Interface Configurations

The types of configurations available for each interface type are shown in the following table.

If you have selected:	You can add a:
An Ethernet interface	• PPPoE connection • Tunnel interface • Loopback interface
Any of the following: • Ethernet with a PPPoE connection • Dialer Interface associated with an ADSL or G.SHDSL configuration • Serial interface with a PPP or HDLC configuration • Serial subinterface with a Frame Relay configuration • Unsupported WAN interface	• Tunnel interface • Loopback Interface

An ATM interface without any encapsulation	• An ADSL interface • A G.SHDSL interface • A tunnel or loopback for either of the above
A serial interface	• A Frame Relay connection • A PPP connection • A tunnel interface • A loopback interface
ATM subinterface An Ethernet subinterface A dialer interface not associated with an ATM interface A loopback A tunnel	• A tunnel interface • A loopback interface

DHCP Address Pools

The IP addresses that the DHCP server assigns are drawn from a common pool that you configure by specifying the starting IP address in the range and the ending address in the range.

The address range that you specify should be within the following private address ranges:

- 10.1.1.1 to 10.255.255.255
- 172.16.1.1 to 172.31.255.255

The address range that you specify must also be in the same subnet as the IP address of the LAN interface. The range can represent a maximum of 254 addresses. The following examples are valid ranges:

- 10.1.1.1 to 10.1.1.254 (assuming LAN IP address is in 10.1.1.0 subnet)
- 172.16.1.1 to 172.16.1.254 (assuming LAN IP address is in 172.16.1.0 subnet)

Cisco SDM configures the router to automatically exclude the LAN interface IP address in the pool.

Reserved Addresses

You must not use the following addresses in the range of addresses that you specify:

- The network/subnetwork IP address.
- The broadcast address on the network.

Meanings of the Permit and Deny Keywords

Rule entries can be used in access rules, NAT rules, IPSec rules, and in access rules associated with route maps. Permit and Deny have various meanings depending on which type of rule is using it.

Rule Type	Meaning of Permit	Meaning of Deny
Access rule	Allow matching traffic in or out of the interface to which the rule has been applied.	Drop matching traffic.
NAT rule	Translate the IP address of matching traffic to the specified inside local address or outside local address.	Do not translate the address.
IPSec rule (Extended only)	Encrypt traffic with matching address.	Do not encrypt traffic. Allow it to be sent unencrypted.
Access rule used in route map	Protect matching addresses from NAT translation.	Do not protect matching addresses from NAT translation.

Services and Ports

This topic lists services you can specify in rules, and their corresponding port numbers. It also provides a short description of each service.

This topic is divided into the following areas:

- TCP Services
- UDP Services
- ICMP Message Types

- IP Services
- Services That Can Be Specified in Inspection Rules

TCP Services

TCP Service	Port Number	Description
bgp	179	Border Gateway Protocol.BGP exchanges reachability information with other systems that use the BGP protocol
chargen	19	Character generator.
cmd	514	Remote commands. Similar to exec except that cmd has automatic authentication
daytime	13	Daytime
discard	9	Discard
domain	53	Domain Name Service. System used on the Internet for translating names of etwork nodes into addresses.
echo	7	Echo request. Message sent when ping command is issued.
exec	512	Remote process execution
finger	79	Finger. Application that determines whether a person has an account at a particular internet site.
ftp	21	File Transfer Protocol. Application-layer protocol used for transferring files between network nodes.
ftp-data	20	FTP data connections
gopher	70	Gopher. A distributed document delivery system.
hostname	101	NIC hostname server
ident	113	Ident Protocol
irc	194	Internet Relay Chat. A world-wide protocol that allows users to exchange text messages with each other in real time.
klogin	543	Kerberos login. Kerberos is a developing standard for authenticating network users.
kshell	544	Kerberos shell
login	513	Login

TCP Service	Port Number	Description
lpd	515	Line Printer Daemon. A protocol used to send print jobs between UNIX systems.
nntp	119	Network News Transport Protocol.
pim-auto-rp	496	Protocol-Independent Multicast Auto-RP. PIM is a multicast routing architecture that allows the addition of multicast IP routing on existing IP networks.
pop2	109	Post Office Protocol v2. Protocol that client e-mail applications use to retrieve mail from mail servers.
pop3	110	Post Office Protocol v3
smtp	25	Simple Mail Transport Protocol. Internet protocol providing e-mail services.
sunrpc	111	SUN Remote Procedure Call. See rpc.
syslog	514	System log.

UDP Services

UDP Service	Port Number	Description
biff	512	Used by mail system to notify users that new mail is received
bootpc	69	Bootstrap Protocol (BOOTP) client
bootps	67	Bootstrap Protocol (BOOTP) server
discard	9	Discard
dnsix	195	DNSIX security protocol auditing
domain	53	Domain Name Service (DNS)
echo	7	See echo.
isakmp	500	Internet Security Association and Key Management Protocol
mobile-ip	434	Mobile IP registration
nameserver	42	IEN116 name service (obsolete)
netbios-dgm	138	NetBios datagram service. Network Basic Input Output System. An API used by applications to request services from lower-level network processes.

UDP Service	Port Number	Description
netbios-ns	137	NetBios name service
netbios-ss	139	NetBios session service
ntp	123	Network Time Protocol. TCP protocol that ensures accurate local timekeeping with reference to radio and atomic clocks located on the Internet.
pim-auto-rp	496	Protocol Independent Multicast, reverse path flooding, dense mode
rip	520	Routing Information Protocol. A protocol used to exchange route information between routers.
snmp	161	Simple Network Management Protocol. A protocol used to monitor and control network devices.
snmptrap	162	SNMP trap. A system management notification of some event that occurred on the remotely managed system.
sunrpc	111	SUN Remote Procedure Call. RPCs are procedure calls that are built or specified by clients and executed on servers, with the results returned over the network to the client.
syslog	514	System log service.
tacacs	49	Terminal Access Controller Access Control System. Authentication protocol that provides remote access authentication and related services, such as logging.
talk	517	Talk. A protocol originally intended for communication between teletype terminals, but now a rendezvous port from which a TCP connection can be established.
tftp	69	Trivial File Transfer Protocol. Simplified version of FTP that allows files to be transferred between network nodes.
time	37	Time.
who	513	Port to databases showing who is logged in to machines on a local net and the load average of the machine
xdmcp	177	X-Display Manager Client Protocol. A protocol used for communications between X-Displays (clients) and X Display Managers.
non500-isakmp	4500	Internet Security Association and Key Management Protocol. This keyword is used when NAT-traversal port floating is required.

ICMP Message Types

ICMP Messages	Port Number	Description
alternate-address	6	Alternate host address.
conversion-error	31	Sent to report a datagram conversion error.
echo	8	Type of message sent when ping command is issued.
echo-reply	0	Response to an echo-request (ping) message.
information-reply	16	Obsolete. Response to message sent by host to discover number of the network it is on. Replaced by DHCP.
information-request	15	Obsolete. Message sent by host to discover number of the network it is on. Replaced by DHCP.
mask-reply	18	Response to message sent by host to discover network mask for the network it is on.
mask-request	17	Obsolete. Message sent by host to discover network mask for the network it is on.
mobile-redirect	32	Mobile host redirect. Sent to inform a mobile host of a better first-hop node on the path to a destination.
parameter-problem	12	Message generated in response to packet with problem in its header.
redirect	5	Sent to inform a host of a better first-hop node on the path to a destination.
router-advertisement	9	Sent out periodically, or in response to a router solicitation.
router-solicitation	10	Messages sent in order to prompt routers to generate router advertisements messages quickly.
source-quench	4	Sent when insufficient buffer space is available to queue packets for transmission to next hop, or by destination router when packets are arriving too quickly to be processed.
time-exceeded	11	Sent to indicate received packet’t time to live field has reached zero.
timestamp-reply	14	Reply to request for timestamp to be used for synchronization between two devices.

ICMP Messages	Port Number	Description
timestamp-request	13	Request for timestamp to be used for synchronization between two devices.
traceroute	30	Message sent in reply to a host that has issued a traceroute request.
unreachable	3	Destination unreachable. Packet cannot be delivered for reasons other than congestion.

IP Services

IP Services	Port Number	Description
aahp	51	
eigrp	88	Enhanced Interior Gateway Routing Protocol. Advanced version of IGRP developed by Cisco.
esp	50	Extended Services Processor.
icmp	1	Internet Control Message Protocol. Network layer protocol that reports errors and provides other information relevant to IP packet processing.
igmp	2	Internet Group Management Protocol. Used by IP hosts to report their multicast group memberships to adjacent multicast routers.
ip	0	Internet Protocol. Network layer protocol offering connectionless internetwork service.
ipinip	4	IP-in-IP encapsulation.
nos	94	network operating system. A distributed file system protocol.
ospf	89	Open Shortest Path First. A link-state hierarchical routing algorithm.
pcp	108	Payload Compression Protocol
pim	103	Protocol-Independent Multicast. PIM is a multicast routing architecture that allows the addition of multicast IP routing on existing IP networks.

IP Services	Port Number	Description
tcp	6	Transmission Control Protocol. Connection-oriented transport layer protocol that provides reliable full-duplex data transmission.
udp	17	User Datagram Protocol. Connectionless transport layer protocol in the TCP/IP protocol stack.

Services That Can Be Specified in Inspection Rules

Protocol	Description
cuseeme	Videoconferencing protocol.
fragment	Specifies that the rule perform fragment inspection.
ftp	See ftp.
h323	See H.323.
http	See HTTP.
icmp	See icmp.
netshow	NetShow. A streaming video protocol.
rcmd	Remote Comman d. A protocol used when commands are executed on a remote system by a local system.
realaudio	RealAudio. A streaming audio protocol.
rpc	Remote Procedure Call. RPCs are procedure calls that are built or specified by clients and executed on servers, with the results returned over the network to the client
rtsp	Real-Time Streaming Protocol. An application-level protocol used to control delivery of data with real-time properties.
sip	Session Initiation Protocol. Sip is a telephony protocol used to integrate telephony services and data services.
skinny	A telephony protocol enabling telephony clients to be H.323 compliant.
smtp	See smtp.
sqlnet	Protocol for network enabled databases.
streamworks	StreamWorks protocol. Streaming video protocol.

Protocol	Description
tcp	See tcp.
tftp	See tftp.
udp	See udp.
vdolive	VDOLive protocol. A streaming video protocol.

More About NAT

This section provides scenario information that may help you in completing the NAT Translation Rule windows, and other information that explains why NAT rules created using the CLI may not be editable in Cisco SDM.

Static Address Translation Scenarios

The following scenarios show you how you can use the static address translation rules.

Scenario 1

You need to map an IP address for a single host to a public address. The address of the host is 10.12.12.3. The public address is 172.17.4.8.

The following table shows how the fields in the Add Address Translation Rule window would be used.

	Translate from Interface Fields		Translate to Interface Fields	
Static/Dynamic	IP Address	Net Mask	IP Address	Redirect Port
Static	10.12.12.3	Leave blank	172.17.4.8	Leave unchecked.

Result

The source address 10.12.12.3 is translated to the address 172.17.4.8 in packets leaving the router. If this is the only NAT rule for this network, 10.12.12.3 is the only address on the network that gets translated.

Scenario 2

You need to map each IP address in a network to a unique public IP address, and you do not want to create a separate rule for each mapping. The source network number is 10.l2.12.0, and the target network is 172.17.4.0. However, in this scenario, it is not necessary to know the source or target network numbers. It is sufficient to enter host addresses and a network mask.

The following table shows how the fields in the Add Address Translation Rule window would be used.

	Translate from Interface Fields		Translate to Interface Fields	
Static/Dynamic	**IP Address**	**Net Mask**	**IP Address**	**Redirect Port**
Static	10.12.12.35 (host)	255.255.255.0	172.17.4.8 (host)	Leave unchecked.

Result

NAT derives the “Translate from” network address from the host IP address and the subnet mask. NAT derives the “Translate to” network address from the the net mask entered in the “Translate from” fields, and the “Translate to” IP address. The source IP address in any packet leaving the original network is translated to an address in the 172.17.4.0 network.

Scenario 3

You want to use the same global IP address for several hosts on the trusted network. Inbound traffic will contain a different port number based on the destination host.

The following table shows how the fields in the Add Address Translation Rule window would be used.

	Translate from... fields		Translate to... fields	
Static/Dynamic	**IP Address**	**Net Mask**	**IP Address**	**Redirect Port**
Static	10.12.12.3	Leave blank	172.17.4.8	UDP Original Port 137 Translated Port 139

Result

The source address 10.12.12.3 is translated to the address 172.17.4.8 in packets leaving the router. The port number in the Redirect port field is changed from 137 to 139. Return traffic carrying the destination address 172.17.4.8 is routed to port number 137 of the host with the IP address 10.12.12.3.

You need to create a separate entry for each host/port mapping that you want to create. You can use the same "Translated to" IP address in each entry, but you must enter a different "Translated from" IP address in each entry, and a different set of port numbers.

Scenario 4

You want source-"Translate from"-addresses to use the IP address that is assigned to the router's Fast Ethernet 0/1 interface 172.17.4.8. You also want to use the same global IP address for several hosts on the trusted network. Inbound traffic will contain a different port number based on the destination host. The following table shows how the fields in the Add Address Translation Rule window would be used:

	Translate from... fields		Translate to... fields	
Static/Dynamic	IP Address	Net Mask	IP Address	Redirect Port
Static	10.12.12.3	Leave blank	FastEthernet 0/1	UDP Original Port 137 Translated Port 139

Result

The source address 10.12.12.3 is translated to the address 172.17.4.8 in packets leaving the router. The port number in the Redirect port field is changed from 137 to 139. Return traffic carrying the destination address 172.17.4.8 & port 139 is routed to port number 137 of the host with the IP address 10.12.12.3.

Dynamic Address Translation Scenarios

The following scenarios show you how you can use dynamic address translation rules. These scenarios are applicable whether you select from inside-to-outside, or from outside-to-inside.

Scenario 1

You want source–"Translate from"–addresses to use the IP address that is assigned to the router's Fast Ethernet 0/1 interface 172.17.4.8. Port Address Translation (PAT) would be used to distinguish traffic associated with different hosts. The ACL rule you use to define the "Translate from" addresses is configured as shown below:

```
access-list 7 deny host 10.10.10.1
access-list 7 permit 10.10.10.0 0.0.0.255
```

When used in a NAT rule this access rule would allow any host in the 10.10.10.0 network, except the one with the address 10.10.10.1 to receive address translation.

The following table shows how the fields in the Add Address Translation Rule window would be used.

	Translate from... fields	**Translate to... fields**		
Static/Dynamic	**ACL Rule**	**Type**	**Interface**	**Address Pool**
Dynamic	7	Interface	FastEthernet0/1	Disabled

Result

Traffic from all hosts on the 10.10.10.0 network would have the source IP address translated to 172.17.4.8. PAT would be used to distinguish traffic associated with different hosts.

Scenario 2

You want the host addresses specified in access-list 7 in the previous scenario to use addresses from a pool you define. If the addresses in the pool become depleted, you want the router to use PAT to satisfy additional requests for addresses from the pool.

The following table shows how the fields in the Address Pool window would be used for this scenario.

Pool Name	Port Address Translation	IP Address fields		Network Mask
Pool 1	Checked	172.16.131.2	172.16.131.10	255.255.255.0

The following table shows how the fields in the Add Address Translation Rule window would be used for this scenario.

	Translate from... fields	Translate to... fields		
Static/Dynamic	ACL Rule	Type	Interface	Address Pool
Dynamic	7	Address Pool	Disabled	Pool 1

Result

Hosts IP addresses in the network 10.10.10.0 are translated to IP address in the range 172.16.131.2 to 172.16.131.10. When there are more requests for address translation than available addresses in Pool 1, the same address is used to satisfy subsequent requests, and PAT is used to distinguish between the hosts using the address.

Reasons that Cisco SDM Cannot Edit a NAT Rule

A previously configured NAT rule will be read-only and will not be configurable when a NAT static rule is configured with any of the following:

- The **inside source static** and **destination** Cisco IOS commands

- The **inside source static network** command with one of the keywords “extendable”, “no-alias”, or “no-payload”
- The **outside source static network** command with one of the keywords “extendable”, “no-alias”, or “no-payload”
- The **inside source static tcp** command with one of the keywords “no-alias” or “no-payload”
- The **inside source static udp** command with one of the keywords “no-alias” or “no-payload”
- The **outside source static tcp** command with one of the keywords “no-alias” or “no-payload”
- The **outside source static udp** command with one of the keywords “no-alias” or “no-payload”
- The **inside source static** command with one of the keywords “no-alias”, “no-payload”, “extendable”, “redundancy”, “route-map”, or “vrf”
- The **outside source static** command with one of the keywords “no-alias”, “no-payload”, “extendable”, or “add-route”
- The **inside source static** command with the keyword “esp”
- The **inside source static** command with the **interface** command

A NAT dynamic rule is configured with the Loopback interface

More About VPN

These topics contain more information about VPN, DMVPN, IPSec and IKE.

Cisco.com Resources

The following links provide TAC resources and other information on VPN issues.

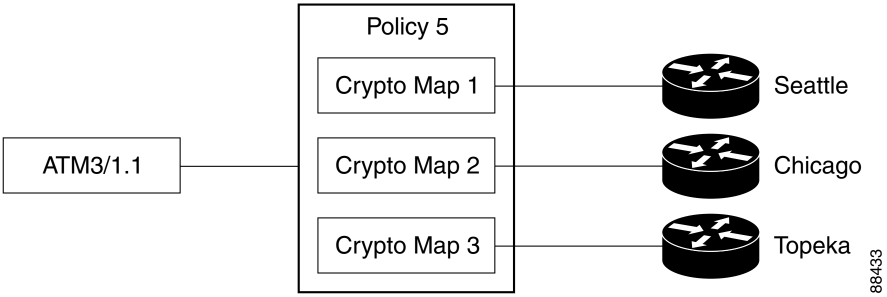
- How Virtual Private Networks Work
- Dynamic Multipoint IPSec VPNs
- TAC-authored articles on IPSec
- TAC-authored articles on Cisco SDM

- Security and VPN Devices
- IPSecurity Troubleshooting–Understanding and Using Debug Commands
- Field Notices

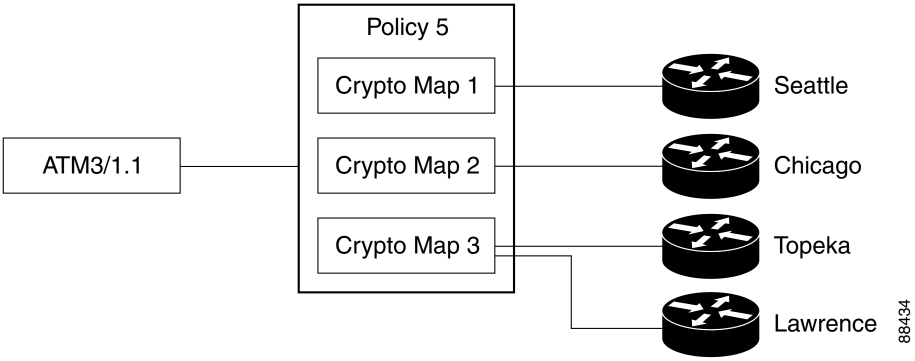
More about VPN Connections and IPSec Policies

A VPN connection is an association between a router interface and an IPSec policy. The building block of an IPSec policy is the crypto map. A crypto map specifies the following: a transform set and other parameters to govern encryption, the identity of one or more peers, and an IPSec rule that specifies which traffic will be encrypted. An IPSec policy can contain multiple crypto maps.

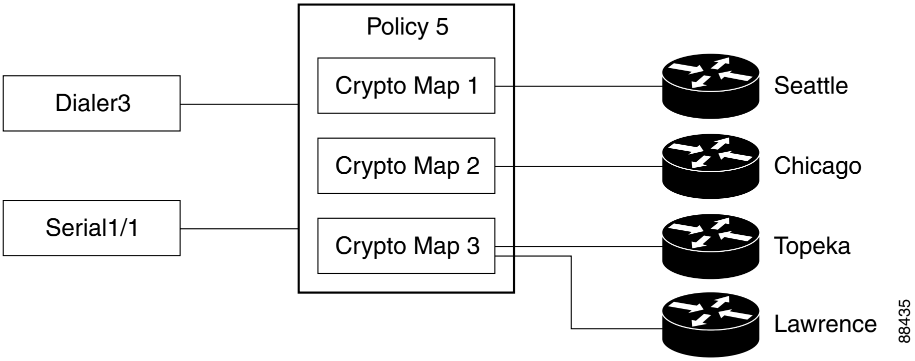
The following diagram shows an interface (ATM 3/1.1) associated with an IPSec policy. The policy has three crypto maps, each specifying a different peer system. The ATM 3/1.1 interface is thus associated with three VPN connections.



A crypto map can specify more than one peer for a connection. This may be done to provide redundancy. The following diagram shows the same interface and policy, but crypto map CM-3 specifies two peers: Topeka and Lawrence.



A router interface can be associated with only one IPSec policy. However, an IPSec policy can be associated with multiple router interfaces, and a crypto map can specify more than one peer for a connection. The following diagram shows two router interfaces associated with a policy, and a crypto map specifying two peers.



There are six VPN connections in this configuration, as both Dialer 3 and Serial 1/1 have connections to Seattle, Chicago, Topeka, and Lawrence. Cisco SDM would show the links to Topeka and Lawrence as one connection for both interfaces.

More About IKE

IKE handles the following tasks:

- Authentication
- Session Negotiation
- Key Exchange
- IPSec Tunnel Negotiation and Configuration

Authentication

Authentication is arguably the most important task that IKE accomplishes, and it certainly is the most complicated. Whenever you negotiate something, it is of utmost importance that you know with whom you are negotiating. IKE can use one of several methods to authenticate negotiating parties to each other.

- **Pre-shared Key**. IKE uses a hashing technique to ensure that only someone who possesses the same key could have sent the IKE packets.
- **DSS or RSA digital signatures**. IKE uses public-key digital-signature cryptography to verify that each party is whom he or she claims to be.
- **RSA encryption**. IKE uses one of two methods to encrypt enough of the negotiation to ensure that only a party with the correct private key could continue the negotiation.

Note Cisco SDM supports the pre-shared key method of authentication.

Session Negotiation

During session negotiation, IKE allows parties to negotiate how they will conduct authentication and how they will protect any future negotiations (that is, IPSec tunnel negotiation). The following items are negotiated:

- **Authentication Method**. This is one of the authentication methods listed above.
- **Key Exchange Algorithm**. This is a mathematical technique for securely exchanging cryptographic keys over a public medium (that is, Diffie-Hellman). The keys are used in the encryption and packet-signature algorithms.

- **Encryption Algorithm**: DES, 3DES, or AES
- **Packet Signature Algorithm**: MD5 or SHA-1

Key Exchange

IKE uses the negotiated key-exchange method (see “Session Negotiation” above) to create enough bits of cryptographic keying material to secure future transactions. This method ensures that each IKE session will be protected with a new, secure set of keys.

Authentication, session negotiation, and key exchange constitute phase 1 of an IKE negotiation.

IPSec Tunnel Negotiation and Configuration

After IKE has finished negotiating a secure method for exchanging information (phase 1), we use IKE to negotiate an IPSec tunnel. This is accomplished in IKE phase 2. In this exchange, IKE creates fresh keying material for the IPSec tunnel to use (either using the IKE phase 1 keys as a base or by performing a new key exchange). The encryption and authentication algorithms for this tunnel are also negotiated.

More About IKE Policies

When the IKE negotiation begins, IKE looks for an IKE policy that is the same on both peers. The peer that initiates the negotiation will send all its policies to the remote peer, and the remote peer will try to find a match. The remote peer looks for a match by comparing its own highest priority policy against the other peer’s received policies. The remote peer checks each of its policies in order of its priority (highest first) until a match is found.

A match is made when both policies from the two peers contain the same encryption, hash, authentication, and Diffie-Hellman parameter values, and when the remote peer’s policy specifies a lifetime less than or equal to the lifetime in the policy being compared. If the lifetimes are not identical, the shorter lifetime-from the remote peer’s policy will be used.

Allowable Transform Combinations

To define a transform set, you specify one to three transforms. Each transform represents an IPSec security protocol (AH or ESP) plus the algorithm that you want to use. When the particular transform set is used during negotiations for IPSec security associations, the entire transform set (the combination of protocols, algorithms, and other settings) must match a transform set at the remote peer.

The following table lists the acceptable transform combination selections for the AH and ESP protocols.

AH Transform (***Pick up to one***)	**ESP Encryption Transform** (***Pick up to one***)	**Authentication Transform** (***Pick up to one***)	**IP Compression Transform** (***Pick up to one***)	**Examples** *(Total of 3 transforms allowed)*
ah-md5-hmac ah-sha-hmac	esp-des esp-3des esp-null es-aes-128 esp-aes-192 esp-aes-256 esp-seal	esp-md5-hmac esp-sha-hmac	comp-lzs	**1.** ah-md5-hmac **2.** esp-3des and esp-md5-hmac **3.** ah-sha-hmac, esp-des, and esp-sha-hmac

The following table describes each of the transforms.

Transform	Description
ah-md5-hmac	AH with the MD5 (HMAC variant) authentication algorithm.
ah-sha-hmac	AH with the SHA (HMAC variant) authentication algorithm.
esp-des	ESP with the 56-bit DES encryption algorithm.
esp-3des	ESP with the 168-bit DES encryption algorithm (3DES or Triple DES)
esp-null	Null encryption algorithm.
esp-seal	ESP with the 160-bit encryption key Software Encryption Algorithm (SEAL) encryption algorithm.

Transform	Description
esp-md5-hmac	ESP with the MD5 (HMAC variant) authentication algorithm.
es-aes-128	ESP with Advanced Encryption Standard (AES). Encryption with a 128-bit key
esp-aes-192	ESP with AES. Encryption with a 192-bit key.
esp-aes-256	ESP with AES. Encryption with a 256-bit key.
esp-sha-hmac	ESP with the SHA (HMAC variant) authentication algorithm.
comp-lzs	IP compression with the LZS algorithm.

Examples

The following are examples of permissible transform combinations:

- ah-md5-hmac
- esp-des
- esp-3des and esp-md5-hmac
- ah-sha-hmac, esp-des, and esp-sha-hmac
- comp-lzs

Reasons Why a Serial Interface or Subinterface Configuration May Be Read-Only

A previously configured Serial interface or subinterface will be read-only and will not be configurable in the following cases:

- The interface is configured with the **encapsulation ppp** and **ppp multilink ...** Cisco IOS commands.
- The interface is configured with the **encapsulation hdlc** and **ip address negotiated** commands.
- The interface is part of a SERIAL_CSUDSU_56K WIC.
- The interface is part of a Sync/Async WIC configured with the **physical-layer async** command.

- The interface is configured with the **encapsulation frame-relay** command with an IP address on the main interface.
- The interface encapsulation is not “hdlc,” “ppp,” or “frame-relay.”
- The **encapsulation frame-relay ...** command contains the **mfr ...** option.
- The interface is configured with the **encapsulation ppp** command, but the PPP configuration contains unsupported commands.
- The interface is configured with the **encapsulation frame-relay** and **frame-relay map ...** commands.
- The main interface is configured with the **encapsulation frame-relay** and **frame-relay interface-dlci ...** commands.
- The main interface is configured with the **encapsulation frame-relay** command and the subinterface is configured with the **frame-relay priority-dlci-group ...** command.
- The subinterface is configured with the **interface-dlci ...** command that contains any of the keywords “ppp,” “protocol,” or “switched.”
- The subinterface type is “multipoint,” instead of “point-to-point.”
- The subinterface is configured with any encapsulation other than “frame-relay.”

Reasons Why an ATM Interface or Subinterface Configuration May Be Read-Only

A previously configured ATM interface or subinterface will be read-only and will not be configurable in the following cases:

- It has a PVC with the **dialer pool-member** command.
- It has a PVC in which the protocol specified in the **protocol** command is not **ip.**
- It has a PVC with multiple **protocol ip** commands.
- The encapsulation on the PVC is neither “aal5mux,” nor “aal5snap.”
- If the encapsulation protocol on aal5mux is not “ip.”
- If the IP Address is not configured on the PVC in the **protocol ip** command.

- If the “dial-on-demand” option is configured on the **pppoe-client** command.
- If there is more than 1 PVC configured on the interface.
- If the encapsulation on the associated dialer is blank or is not “ppp.”
- If no IP address is configured on the associated dialer.
- If VPDN is required (which is determined dynamically from the Cisco IOS image) but is not configured for this connection.
- If the operating mode is “CO” on an SHDSL interface (ATM main interfaces only).
- If no IP address is configured on the interface and the interface is not configured for PPPoE (ATM subinterfaces only).
- The interface has an IP address but no associated PVC.
- The interface has a PVC but no associated IP address and is not configured for PPPoE.
- The **bridge-group** command is configured on the interface.
- If the main interface has one or move PVCs as well as one or more subinterfaces.
- If the main interface is not configurable (ATM subinterfaces only).
- It is a multipoint interface (ATM subinterfaces only).

Reasons Why an Ethernet Interface Configuration May Be Read-Only

A previously configured Ethernet LAN or WAN interface or will be read-only and will not be configurable in the following cases:

- If the LAN interface has been configured as a DHCP server, and has been configured with an IP-helper address.

Reasons Why an ISDN BRI Interface Configuration May Be Read-Only

A previously configured ISDN BRI interface will be read-only and will not be configurable in the following cases:

- An IP address is assigned to the ISDN BRI interface.
- Encapsulation other than ppp is configured on the ISDN BRI interface.
- The **dialer-group** or **dialer string** command is configured on the ISDN BRI interface.
- **dialer pool-member** <*x*> is configured on the ISDN BRI interface, but the corresponding dialer interface <*x*> is not present.
- Multiple dialer pool-members are configured on the ISDN BRI interface.
- The **dialer map** command is configured on the ISDN BRI interface.
- Encapsulation other than ppp is configured on the dialer interface.
- Either **dialer-group** or **dialer-pool** is not configured on the dialer interface.
- **dialer-group** <*x*> is configured on the dialer interface, but the corresponding **dialer -list** <*x*> **protocol** command is not configured.
- **dialer idle-timeout** <*num*> with optional keyword (either/inbound) is configured on the dialer interface.
- **dialer string** command with optional keyword **class** is configured on the dialer interface.
- If using the ISDN BRI connection as a backup connection, once the backup configuration is through Cisco SDM, if any of the conditions below occur, the backup connection will be shown as read only:
  - The default route through the primary interface is removed
  - The backup interface default route is not configured
  - ip local policy is removed
  - **track /rtr** or **both** is not configured
  - route-map is removed
  - Access-list is removed or access-list is modified (for example, tracking ip address is modified)

- The Cisco SDM-supported interfaces are configured with unsupported configurations
- The primary interfaces are not supported by Cisco SDM

Reasons Why an Analog Modem Interface Configuration May Be Read-Only

A previously configured analog modem interface or will be read-only and will not be configurable in the following cases:

- An IP address is assigned to the asynchronous interface.
- Encapsulation other than ppp is configured on the asynchronous interface.
- The **dialer-group** or **dialer string** command is configured on the asynchronous interface.
- Async mode **interactive** is configured on the asynchronous interface.
- **dialer pool-member** <*x*> is configured on the asynchronous interface, but the corresponding dialer interface <*x*> is not present.
- Multiple dialer pool-members are configured on the asynchronous interface.
- Encapsulation other than ppp is configured on the dialer interface.
- Either **dialer-group** or **dialer-pool** is not configured on the dialer interface.
- **dialer-group** <*x*> is configured on the dialer interface, but the corresponding **dialer -list** <*x*> **protocol** command is not configured.
- **dialer idle-timeout** <*num*> with optional keyword (either/inbound) is configured on the dialer interface.
- In line configuration collection mode, **modem inout** is not configured.
- In line configuration collection mode, **autoselect ppp** is not configured.
- If using the analog modem connection as a backup connection, once the backup configuration is through Cisco SDM, if any of the conditions below occur, the backup connection will be shown as read only:
  - The default route through the primary interface is removed
  - The backup interface default route is not configured
  - ip local policy is removed

- **track /rtr** or **both** is not configured
- route-map is removed
- Access-list is removed or access-list is modified (for example, tracking ip address is modified)
- The Cisco SDM-supported interfaces are configured with unsupported configurations
- The primary interfaces are not supported by Cisco SDM

Firewall Policy Use Case Scenario

For information on firewall policy management, including detailed deployment scenarios, see the document at the following link:

http://www.cisco.com/application/pdf/en/us/guest/products/ps5318/c1225/ccmigration_09186a0080230754.pdf

DMVPN Configuration Recommendations

This help topic contains recommendations on how you should proceed when configuring routers in a DMVPN.

Configure the Hub First

It is important to configure the hub first because spokes must be configured using information about the hub. If you are configuring a hub, you can use the Spoke Configuration feature available in the Summary window to generate a text file that contains a procedure that you can send to spoke administrators so that they can configure the spokes with the correct hub information. If you are configuring a spoke, you must obtain the correct information about the hub before you begin.

Assigning Spoke Addresses

All routers in the DMVPN must be in the same subnet. Therefore, the hub administrator must assign addresses in the subnet to the spoke routers so that address conflicts do not occur, and so that everyone is using the same subnet mask.

Recommendations for Configuring Routing Protocols for DMVPN

The following are guidelines that you should note when configuring routing protocols for DMVPN. You can choose to ignore these guidelines, but Cisco SDM has not been tested in scenarios outside the guidelines and may not be able to let you edit configurations within Cisco SDM after you enter them.

These recommendations are listed in best-choice order:

- If a routing process exists that advertises inside networks, use this process to advertise networks to the DMVPN.
- If a routing process exists that advertises tunnel networks for VPNs, for example GRE over IPSec tunnels, use this process to advertise the DMVPN networks.
- If a routing process exists that advertises networks for the WAN interfaces, then be sure to use an AS number or process ID that the WAN interfaces do not use to advertise networks.
- When you configure DMVPN routing information Cisco SDM checks whether the Autonomous System number (EIGRP) or area ID (OSPF) you enter is already used to advertise networks for the router's physical interface. If the value is already in use, Cisco SDM informs you of this and recommends that you either use a new value, or that you select a different routing protocol to advertise networks on the DMVPN.

Using Interfaces with Dialup Configurations

Selecting an interface that uses a dialup connection may cause the connection to be always up. You can examine supported interfaces in Interfaces and Connections to determine if a dialup connection, such as an ISDN or Async connection has been configured for the physical interface you selected.

Ping the Hub Before You Start Spoke Configuration

Before configuring a spoke router, you should test connectivity to the hub by issuing the ping command. If the ping does not succeed, you must configure a route to the hub.

Cisco SDM White Papers

A number of white papers are available that describe how Cisco SDM can be used. These white papers are available at the following link.

http://www.cisco.com/univercd/cc/td/doc/product/software/sdm/appnote/index.htm