

crypto dynamic-map

To create a dynamic crypto map entry and enter the crypto map configuration command mode, use the **crypto dynamic-map** command in global configuration mode. To delete a dynamic crypto map set or entry, use the **no** form of this command.

crypto dynamic-map *dynamic-map-name* *dynamic-seq-num*

no crypto dynamic-map *dynamic-map-name* [*dynamic-seq-num*]

Syntax Description

<i>dynamic-map-name</i>	Specifies the name of the dynamic crypto map set.
<i>dynamic-seq-num</i>	Specifies the number of the dynamic crypto map entry.

Defaults

No dynamic crypto maps exist.

Command Modes

Global configuration.

Command History

Release	Modification
11.3 T	This command was introduced.

Usage Guidelines

Use dynamic crypto maps to create policy templates that can be used when processing negotiation requests for new security associations from a remote IP Security peer, even if you do not know all of the crypto map parameters required to communicate with the remote peer (such as the peer's IP address). For example, if you do not know about all the IPSec remote peers in your network, a dynamic crypto map allows you to accept requests for new security associations from previously unknown peers. (However, these requests are not processed until the Internet Key Exchange authentication has completed successfully.)

When a router receives a negotiation request via IKE from another IPSec peer, the request is examined to see if it matches a crypto map entry. If the negotiation does not match any explicit crypto map entry, it will be rejected unless the crypto map set includes a reference to a dynamic crypto map.

The dynamic crypto map is a policy template; it will accept "wildcard" parameters for any parameters not explicitly stated in the dynamic crypto map entry. This allows you to set up IPSec security associations with a previously unknown IPSec peer. (The peer still must specify matching values for the "non-wildcard" IPSec security association negotiation parameters.)

If the router accepts the peer's request, at the point that it installs the new IPSec security associations it also installs a temporary crypto map entry. This entry is filled in with the results of the negotiation. At this point, the router performs normal processing, using this temporary crypto map entry as a normal entry, even requesting new security associations if the current ones are expiring (based upon the policy specified in the temporary crypto map entry). Once the flow expires (that is, all of the corresponding security associations expire), the temporary crypto map entry is removed.

Dynamic crypto map sets are not used for initiating IPSec security associations. However, they are used for determining whether or not traffic should be protected.

The only configuration required in a dynamic crypto map is the **set transform-set** command. All other configuration is optional.

Dynamic crypto map entries, like regular static crypto map entries, are grouped into sets. After you define a dynamic crypto map set (which commonly contains only one map entry) using this command, you include the dynamic crypto map set in an entry of the “parent” crypto map set using the **crypto map** (IPSec global configuration) command. The parent crypto map set is then applied to an interface.

You should make crypto map entries referencing dynamic maps the lowest priority map entries, so that negotiations for security associations will try to match the static crypto map entries first. Only after the negotiation request does not match any of the static map entries do you want it to be evaluated against the dynamic map.

To make a dynamic crypto map the lowest priority map entry, give the map entry referencing the dynamic crypto map the highest *seq-num* of all the map entries in a crypto map set.

For both static and dynamic crypto maps, if unprotected inbound traffic matches a **permit** statement in an access list, and the corresponding crypto map entry is tagged as “IPSec,” then the traffic is dropped because it is not IPSec-protected. (This is because the security policy as specified by the crypto map entry states that this traffic must be IPSec-protected.)

For static crypto map entries, if outbound traffic matches a **permit** statement in an access list and the corresponding security association (SA) is not yet established, the router will initiate new SAs with the remote peer. In the case of dynamic crypto map entries, if no SA existed, the traffic would simply be dropped (because dynamic crypto maps are not used for initiating new SAs).



Note

Use care when using the **any** keyword in **permit** entries in dynamic crypto maps. If it is possible for the traffic covered by such a **permit** entry to include multicast or broadcast traffic, the access list should include **deny** entries for the appropriate address range. Access lists should also include **deny** entries for network and subnet broadcast traffic, and for any other traffic that should not be IPSec protected.

Examples

The following example configures an IPSec crypto map set.

Crypto map entry “mymap 30” references the dynamic crypto map set “mydynamicmap,” which can be used to process inbound security association negotiation requests that do not match “mymap” entries 10 or 20. In this case, if the peer specifies a transform set that matches one of the transform sets specified in “mydynamicmap,” for a flow “permitted” by the access list 103, IPSec will accept the request and set up security associations with the remote peer without previously knowing about the remote peer. If accepted, the resulting security associations (and temporary crypto map entry) are established according to the settings specified by the remote peer.

The access list associated with “mydynamicmap 10” is also used as a filter. Inbound packets that match a **permit** statement in this list are dropped for not being IPSec protected. (The same is true for access lists associated with static crypto maps entries.) Outbound packets that match a **permit** statement without an existing corresponding IPSec SA are also dropped.

```
crypto map mymap 10 ipsec-isakmp
 match address 101
  set transform-set my_t_set1
  set peer 10.0.0.1
  set peer 10.0.0.2
crypto map mymap 20 ipsec-isakmp
 match address 102
  set transform-set my_t_set1 my_t_set2
  set peer 10.0.0.3
```

```

crypto map mymap 30 ipsec-isakmp dynamic mydynamicmap
!
crypto dynamic-map mydynamicmap 10
  match address 103
  set transform-set my_t_set1 my_t_set2 my_t_set3

```

Related Commands	Command	Description
	crypto map (global IPSec)	Creates or modifies a crypto map entry and enters the crypto map configuration mode.
	crypto map (interface IPSec)	Applies a previously defined crypto map set to an interface.
	crypto map local-address	Specifies and names an identifying interface to be used by the crypto map for IPSec traffic.
	match address (IPSec)	Specifies an extended access list for a crypto map entry.
	set peer (IPSec)	Specifies an IPSec peer in a crypto map entry.
	set pfs	Specifies that IPSec should ask for perfect forward secrecy (PFS) when requesting new security associations for this crypto map entry, or that IPSec requires PFS when receiving requests for new security associations.
	set security-association lifetime	Overrides (for a particular crypto map entry) the global lifetime value, which is used when negotiating IPSec security associations.
	set transform-set	Specifies which transform sets can be used with the crypto map entry.
	show crypto engine accelerator logs	Displays a dynamic crypto map set.
	show crypto map (IPSec)	Displays the crypto map configuration.

crypto engine accelerator

To enable the onboard hardware accelerator of the router for IP security (IPSec) encryption, use the **crypto engine accelerator** command in global configuration mode. To disable the use of the onboard hardware IPSec accelerator, and thereby perform IPSec encryption or decryption in software, use the **no** form of this command.

crypto engine accelerator

no crypto engine accelerator

Syntax Description This command has no arguments or keywords.

Defaults The hardware accelerator for IPSec encryption is enabled.

Command Modes Global configuration

Command History	Release	Modification
	12.1(3)T	This command was introduced for the Cisco 1700 series router and other Cisco routers that support hardware accelerators for IPSec encryption.
	12.1(3)XL	Support was added for the Cisco uBR905 cable access router.
	12.2(2)XA	Support was added for the Cisco uBR925 cable access router.
	12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T and implemented for the AIM-VPN/EPII and AIM-VPN/HPII on the following platforms: Cisco 2691, Cisco 3660, Cisco 3725, and Cisco 3745.

Usage Guidelines This command is not normally needed for typical operations because the onboard hardware accelerator of the router is enabled for IPSec encryption by default. The hardware accelerator should not be disabled except on instruction from Cisco Technical Assistance Center (TAC) personnel.

Examples The following example shows how to disable the onboard hardware accelerator of the router for IPSec encryption. This is normally needed only after the accelerator has been disabled for testing or debugging purposes.

```
Router(config)# no crypto engine accelerator
```

```
Warning! all current connections will be torn down.
Do you want to continue? [yes/no]:
```

Related Commands	Command	Description
	clear crypto engine accelerator counter	Resets the statistical and error counters for the hardware accelerator to zero.
	crypto ca	Defines the parameters for the certification authority used for a session.
	crypto cisco	Defines the encryption algorithms and other parameters for a session.
	crypto dynamic-map	Creates a dynamic map crypto configuration for a session.
	crypto ipsec	Defines the IPSec security associations and transformation sets.
	crypto isakmp	Enables and defines the IKE protocol and its parameters.
	crypto key	Generates and exchanges keys for a cryptographic session.
	crypto map	Creates and modifies a crypto map for a session.
	debug crypto engine accelerator control	Displays each control command as it is given to the crypto engine.
	debug crypto engine accelerator packet	Displays information about each packet sent for encryption and decryption.
	show crypto engine accelerator ring	Displays the contents of command and transmits rings for the crypto engine.
	show crypto engine accelerator sa-database	Displays the active (in-use) entries in the crypto engine SA database.
	show crypto engine accelerator statistic	Displays the current run-time statistics and error counters for the crypto engine.
	show crypto engine brief	Displays a summary of the configuration information for the crypto engine.
	show crypto engine configuration	Displays the version and configuration information for the crypto engine.
	show crypto engine connections	Displays a list of the current connections maintained by the crypto engine.

crypto identity

To configure the identity of the router with a given list of distinguished names (DNs) in the certificate of the router, use the **crypto identity** command in global configuration mode. To delete all identity information associated with a list of DN, use the **no** form of this command.

crypto identity *name*

no crypto identity *name*

Syntax Description	<i>name</i> Identity of the router, which is associated with the given list of DN.
---------------------------	--

Defaults	If this command is not enabled, the IP address is associated with the identity of the router.
-----------------	---

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	12.2(4)T	This command was introduced.

Usage Guidelines	The crypto identity command allows you to configure the identity of a router with a given list of DN. Thus, when used with the dn and fqdn commands, you can set restrictions in the router configuration that prevent peers with specific certificates, especially certificates with particular DN, from having access to selected encrypted interfaces.
-------------------------	--



Note

The identity of the peer must be the same as the identity in the exchanged certificate.

Examples	The following example shows how to configure a DN-based crypto map:
-----------------	---

```
! The following is an IPsec crypto map (part of IPsec configuration). It can be used only
! by peers that have been authenticated by DN and if the certificate belongs to BigBiz.
crypto map map-to-bigbiz 10 ipsec-isakmp
  set peer 172.21.114.196
  set transform-set my-transformset
  match address 124
  identity to-bigbiz
!
crypto identity to-bigbiz
  dn ou=BigBiz
!
! This crypto map can be used only by peers that have been authenticated by hostname
! and if the certificate belongs to little.com.
```

```
crypto map map-to-little-com 10 ipsec-isakmp
  set peer 172.21.115.119
  set transform-set my-transformset
  match address 125
  identity to-little-com
!
crypto identity to-little-com
  fqdn little.com
!
```

Related Commands

Command	Description
crypto mib ipsec flowmib history failure size	Associates the identity of the router with the DN in the certificate of the router.
fqdn	Associates the identity of the router with the hostname that the peer used to authenticate itself.

crypto ipsec client ezvpn (global)

To create a Cisco Easy VPN Remote configuration and enter the Cisco Easy VPN Remote configuration mode, use the **crypto ipsec client ezvpn** command in global configuration mode. To delete the Cisco Easy VPN Remote configuration, use the **no** form of this command.

crypto ipsec client ezvpn *name*

no crypto ipsec client ezvpn *name*



Note

A separate **crypto ipsec client ezvpn** command exists in interface configuration mode that assigns a Cisco Easy VPN Remote configuration to the interface.

Syntax Description

<i>name</i>	Identifies the Cisco Easy VPN Remote configuration with a unique, arbitrary name.
-------------	---

Defaults

Newly created Cisco Easy VPN Remote configurations default to the **client** mode.

Command Modes

Global configuration

Command History

Release	Modification
12.2(4)YA	This command was introduced on Cisco 806, Cisco 826, Cisco 827, and Cisco 828 routers; Cisco 1700 series routers; and Cisco uBR905 and Cisco uBR925 cable access routers.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(8)YJ	This command was enhanced to enable you to manually establish and terminate an IP Security (IPSec) Virtual Private Network (VPN) tunnel on demand for Cisco 806, Cisco 826, Cisco 827, and Cisco 828 routers; Cisco 1700 series routers; and Cisco uBR905 and Cisco uBR925 cable access routers.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.

Usage Guidelines

The **crypto ipsec client ezvpn** command creates a Cisco Easy VPN Remote configuration and then enters the Cisco Easy VPN Remote configuration mode, at which point you can enter the following subcommands:

- **connect [auto | manual]**—Manually establishes and terminates an IPSec VPN tunnel on demand.
 - **auto**—(Optional) The default setting. The IPSec VPN tunnel is automatically connected when the Cisco Easy VPN Remote feature is configured on an interface.

- **manual**—(Optional) Specifies the manual setting to direct the Cisco Easy VPN Remote Client to wait for a command or application program interface (API) call before attempting to establish the Cisco Easy VPN Remote connection. When the tunnel times out or fails, subsequent connections have to wait for the command to reset to manual or for an API call.
- **default**—Sets the command that follows to its default values.
- **exit**—Exits Cisco Easy VPN configuration mode and returns to global configuration mode.
- **group** *group-name* **key** *group-key*—Specifies the group name and key value for the VPN connection.
- **local-address** *interface-name*—Informs the Cisco Easy VPN Client of the interface that is used to determine the public IP address. This interface is used to source the tunnel. The **local-address** subcommand applies only to the Cisco uBR905 and Cisco uBR925 cable access routers.
 - The value of the *interface-name* argument specifies the interface used for tunnel traffic.

After specifying the local address used to source tunnel traffic, the IP address can be obtained in two ways:

 - The **local-address** subcommand can be used with the **cable-modem dhcp-proxy {interface loopback number} command to obtain a public IP address and to automatically assign it to the loopback interface.**
 - The IP address can be manually assigned to the loopback interface.
- **mode** { **client** | **network-extension** }—Specifies the mode of operation of the VPN of the router:
 - **client**—(the default) Automatically configures the router for Cisco Easy VPN Client mode operation, which uses Network Address Translation (NAT) or Peer Address Translation (PAT) address translations. When the Cisco Easy VPN Remote configuration is assigned to an interface, the router automatically creates the NAT or PAT and access-list configuration needed for the VPN connection.
 - **network-extension**—Specifies that the router should become a remote extension of the enterprise network at the other end of the VPN connection. The PCs that are connected to the router typically are assigned an IP address in the address space of the enterprise network.
- **no**—Removes the command or sets it to its default values.
- **peer** { *ipaddress* | *hostname* }—Sets the peer IP address or host name for the VPN connection. A host name can be specified only when the router has a DNS server available for hostname resolution.



Note The Cisco Easy VPN Remote feature attempts to resolve the host name when the **peer** command is given, not when the VPN tunnel is created. If the host name cannot be resolved at that time, the **peer** command is not accepted.

After configuring the Cisco Easy VPN Remote configuration, use the **exit** command to exit the Cisco Easy VPN Remote configuration mode and return to global configuration mode.



Note

You cannot use the **no crypto ipsec client ezvpn** command to delete a Cisco Easy VPN Remote configuration that is assigned to an interface. You must remove that Cisco Easy VPN Remote configuration from the interface before you can delete the configuration.

Examples

The following example shows a Cisco Easy VPN Remote configuration named “**telecommuter-client**” being created on a Cisco uBR905 or Cisco uBR925 cable access router and being assigned to cable interface 0:

```
Router# configure terminal
Router(config)# crypto ipsec client ezvpn telecommuter-client
Router(config-crypto-ezvpn)# group telecommute-group key secret-telecommute-key
Router(config-crypto-ezvpn)# peer telecommuter-server
Router(config-crypto-ezvpn)# mode client
Router(config-crypto-ezvpn)# exit
Router(config)# interface c0
Router(config-if)# crypto ezvpn telecommuter-client
Router(config-if)# exit
```

**Note**

Specifying the **mode client** option as shown above is optional because this is the default configuration for these options.

The following example shows the Cisco Easy VPN Remote configuration named “**telecommuter-client**” being removed from the interface and then deleted:

```
Router# configure terminal
Router(config)# interface e1
Router(config-if)# no crypto ipsec client ezvpn telecommuter-client
Router(config-if)# exit
Router(config)# no crypto ipsec client ezvpn telecommuter-client
```

Related Commands

Command	Description
crypto ipsec client ezvpn (interface)	Assigns a Cisco Easy VPN Remote configuration to an interface.

crypto ipsec client ezvpn (interface)

To assign a Cisco Easy VPN Remote configuration to an interface, specify whether the interface is outside or inside, and configure multiple outside and inside interfaces, use the **crypto ipsec client ezvpn** command in interface configuration mode. To remove the Cisco Easy VPN Remote configuration from the interface, use the **no** form of this command.

```
crypto ipsec client ezvpn name [outside | inside]
```

```
no crypto ipsec client ezvpn name [outside | inside]
```



Note

A separate **crypto ipsec client ezvpn** command exists in global configuration mode that creates a Cisco Easy VPN Remote configuration.

Syntax Description

<i>name</i>	Specifies the Cisco Easy VPN Remote configuration to be assigned to the interface.
outside	(Optional) Specifies the outside interface of the IP Security (IPSec) client router. This is optional for outside interfaces. You can add up to four outside tunnels for all platforms, one tunnel per outside interfaces.
inside	(Optional) Specifies the inside interface of the IPSec client router. The Cisco 1700 series has no default inside interface, and any inside interface must be configured. The Cisco 800 series routers and Cisco uBR905 and Cisco uBR925 cable access routers have default inside interfaces. However, you can configure any inside interface. You can add up to three inside interfaces for all platforms.

Defaults

The default inside interface is the Ethernet interface on Cisco 800 series routers and Cisco uBR905 and Cisco uBR925 cable access routers.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(4)YA	This command was introduced on Cisco 806, Cisco 826, Cisco 827, and Cisco 828 routers; Cisco 1700 series routers; and Cisco uBR905 and Cisco uBR925 cable access routers.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(8)YJ	This command was enhanced to enable you to configure multiple outside and inside interfaces for Cisco 806, Cisco 826, Cisco 827, and Cisco 828 routers; Cisco 1700 series routers; and Cisco uBR905 and Cisco uBR925 cable access routers.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.

Usage Guidelines

The **crypto ipsec client ezvpn** command assigns a Cisco Easy VPN Remote configuration to an interface, enabling the creation of a Virtual Private Network (VPN) connection over that interface to the specified VPN peer. If the Cisco Easy VPN Remote configuration is configured for the client mode of operation, this also automatically configures the router for network address translation (NAT) or port address translation (PAT) and for an associated access list.

In Cisco IOS Release 12.2(8)YJ, the **crypto ipsec client ezvpn** command was enhanced to allow you to configure multiple outside and inside interfaces. To configure multiple outside and inside interfaces, you must use the **interface interface-name** command to first define the type of interface on the IPSec client router.

- In client mode for the Cisco Easy VPN Client, a single security association (SA) connection is used for encrypting and decrypting the traffic coming from all the inside interfaces. In network extension mode, one SA connection is established for each inside interface.
- When a new inside interface is added or an existing one is removed, all established SA connections are deleted and new ones are initiated.
- Configuration information for the default inside interface is shown with the **crypto ipsec client ezvpn name inside** command. All inside interfaces, whether they belong to a tunnel, are listed in interface configuration mode as an inside interface, along with the tunnel name.

The following Cisco IOS Release 12.2(4)YA restrictions apply to the **crypto ipsec client ezvpn** command:

- The Cisco Easy VPN Remote feature supports only one tunnel, so the **crypto ipsec client ezvpn** command can be assigned to only one interface. If you attempt to assign it to more than one interface, an error message is displayed. You must use the **no** form of this command to remove the configuration from the first interface before assigning it to the second interface.
- The **crypto ipsec client ezvpn** command should be assigned to the outside interface of the NAT or PAT translation. This command cannot be used on the inside NAT or PAT interface. On some platforms, the inside and outside interfaces are fixed.

For example, on Cisco uBR905 and Cisco uBR925 cable access routers, the outside interface is always the cable interface. On Cisco 1700 series routers, the FastEthernet interface defaults to being the inside interface, so attempting to use the **crypto ipsec client ezvpn** command on the FastEthernet interface displays an error message.



Note

You must first use the global configuration version of the **crypto ipsec client ezvpn** command to create a Cisco Easy VPN Remote configuration before assigning it to an interface.

Examples

The following example shows a Cisco Easy VPN Remote configuration named “**telecommuter-client**” being assigned to the cable interface on a Cisco uBR905/uBR925 cable access router:

```
Router# configure terminal
Router(config)# interface c0
Router(config-if)# crypto ipsec client ezvpn telecommuter-client
Router(config-if)# exit
```

The following example first shows an attempt to delete the Cisco Easy VPN Remote configuration named “**telecommuter-client**,” but the configuration cannot be deleted because it is still assigned to an interface. The configuration is then removed from the interface and deleted.

```
Router# configure terminal
Router(config)# no crypto ipsec client ezvpn telecommuter-client
Error: crypto map in use by interface; cannot delete
Router(config)# interface e1
Router(config-if)# no crypto ipsec client ezvpn telecommuter-client
Router(config-if)# exit
Router(config)# no crypto ipsec client ezvpn telecommuter-client
```

Related Commands

Command	Description
crypto ipsec client ezvpn (global)	Creates and modifies a Cisco Easy VPN Remote configuration.

crypto ipsec client ezvpn connect

To connect to a specified IP Security (IPSec) Virtual Private Network (VPN) tunnel in a manual configuration, use the **crypto ipsec client ezvpn connect** command in privileged EXEC mode. To disable the VPN tunnel, use the **no** form of this command.

crypto ipsec client ezvpn connect *name*

no crypto ipsec client ezvpn connect *name*

Syntax Description	<i>name</i> Identifies the IPSec VPN tunnel with a unique, arbitrary name.						
Defaults	No default behavior or values						
Command Modes	Privileged EXEC						
Command History	<table border="1"> <thead> <tr> <th style="border-top: 1px solid black; border-bottom: 1px solid black;">Release</th> <th style="border-top: 1px solid black; border-bottom: 1px solid black;">Modification</th> </tr> </thead> <tbody> <tr> <td style="border-bottom: 1px solid black;">12.2(8)YJ</td> <td style="border-bottom: 1px solid black;">This command was introduced on Cisco 806, Cisco 826, Cisco 827, and Cisco 828 routers; Cisco 1700 series routers; and Cisco uBR905 and Cisco uBR925 cable access routers.</td> </tr> <tr> <td style="border-bottom: 1px solid black;">12.2(15)T</td> <td style="border-bottom: 1px solid black;">This command was integrated into Cisco IOS Release 12.2(15)T.</td> </tr> </tbody> </table>	Release	Modification	12.2(8)YJ	This command was introduced on Cisco 806, Cisco 826, Cisco 827, and Cisco 828 routers; Cisco 1700 series routers; and Cisco uBR905 and Cisco uBR925 cable access routers.	12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
Release	Modification						
12.2(8)YJ	This command was introduced on Cisco 806, Cisco 826, Cisco 827, and Cisco 828 routers; Cisco 1700 series routers; and Cisco uBR905 and Cisco uBR925 cable access routers.						
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.						
Usage Guidelines	<p>This command is used with the connect [auto manual] subcommand. After the manual setting is designated, the Cisco Easy VPN remote waits for a command or application program interface (API) call before attempting to establish the Cisco Easy VPN Remote connection.</p> <p>If the configuration is manual, the tunnel is connected only after the crypto ipsec client ezvpn connect <i>name</i> command is entered in privileged EXEC mode and after the connect [auto manual] subcommand is entered.</p>						
Examples	<p>The following example shows how to connect an IPSec VPN tunnel named “ISP-tunnel” on a Cisco uBR905/uBR925 cable access router:</p> <pre>Router# crypto ipsec client ezvpn connect ISP-tunnel</pre>						
Related Commands	<table border="1"> <thead> <tr> <th style="border-top: 1px solid black; border-bottom: 1px solid black;">Command</th> <th style="border-top: 1px solid black; border-bottom: 1px solid black;">Description</th> </tr> </thead> <tbody> <tr> <td style="border-bottom: 1px solid black;">crypto ipsec client ezvpn (global)</td> <td style="border-bottom: 1px solid black;">Creates and modifies a Cisco Easy VPN Remote configuration.</td> </tr> </tbody> </table>	Command	Description	crypto ipsec client ezvpn (global)	Creates and modifies a Cisco Easy VPN Remote configuration.		
Command	Description						
crypto ipsec client ezvpn (global)	Creates and modifies a Cisco Easy VPN Remote configuration.						

crypto ipsec client ezvpn xauth

To respond to a pending Virtual Private Network (VPN) authorization request, use the **crypto ipsec client ezvpn xauth** command in privileged EXEC mode.

crypto ipsec client ezvpn xauth *name*

Syntax Description	<i>name</i>	Identifies the IP Security (IPSec) VPN tunnel with a unique, arbitrary name. This is required.
--------------------	-------------	--

Defaults No default behavior or values

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(4)YA	This command was introduced on Cisco 806, Cisco 826, Cisco 827, and Cisco 828 routers; Cisco 1700 series routers; and Cisco uBR905 and Cisco uBR925 cable access routers.
	12.2(8)YJ	This command was enhanced to specify an IPSec VPN tunnel for Cisco 806, Cisco 826, Cisco 827, and Cisco 828 routers; Cisco 1700 series routers; and Cisco uBR905 and Cisco uBR925 cable access routers.
	12.2(8)YJ	This command was enhanced to specify an IPSec VPN tunnel for Cisco 806, Cisco 826, Cisco 827, and Cisco 828 routers; Cisco 1700 series routers; and Cisco uBR905 and Cisco uBR925 cable access routers.
	12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.

Usage Guidelines If the tunnel name is not specified, the authorization request is made on the active tunnel. If there is more than one active tunnel, the command fails with an error requesting that you specify the tunnel name.

When making a VPN connection, individual users might also be required to provide authorization information, such as a username or password. When the remote end requires this information, the router displays a message on the console of the router instructing the user to enter the **crypto ipsec client ezvpn xauth** command. The user then uses command-line interface (CLI) to enter this command and to provide the information requested by the prompts that follow after the command has been entered.



Note If the user does not respond to the authentication notification, the message is repeated every 10 seconds.

Examples

The following example shows an example of the user being prompted to enter the **crypto ipsec client ezvpn xauth** command. The user then enters the requested information and continues.

```
Router#  
20:27:39: EZVPN: Pending XAuth Request, Please enter the following command:  
20:27:39: EZVPN: crypto ipsec client ezvpn xauth
```

```
Router# crypto ipsec client ezvpn xauth  
Enter Username and Password: userid  
Password: *****
```

Related Commands

Command	Description
crypto ipsec client ezvpn (interface)	Assigns a Cisco Easy VPN Remote configuration to an interface.

crypto ipsec df-bit (global)

To set the DF bit for the encapsulating header in tunnel mode to all interfaces, use the **crypto ipsec df-bit** command in global configuration mode.

```
crypto ipsec df-bit [clear | set | copy]
```

Syntax Description	clear	set	copy
	Outer IP header will have the DF bit cleared, and the router may fragment the packet to add the IP Security (IPSec) encapsulation.	Outer IP header will have the DF bit set; however, the router may fragment the packet if the original packet had the DF bit cleared.	The router will look in the original packet for the outer DF bit setting. The copy keyword is the default setting.

Defaults The default is **copy**.

Command Modes Global configuration

Command History	Release	Modification
	12.2(2)T	This command was introduced.

Usage Guidelines Use the **crypto ipsec df-bit** command in global configuration mode to configure your router to specify the DF bit in an encapsulated header.

You may want use the **clear** setting for the DF bit when encapsulating tunnel mode IPSec traffic so you can send packets larger than the available maximum transmission unit (MTU) size or if you do not know what the available MTU size is.

If this command is enabled without a specified setting, the router will use the **copy** setting as the default.

Examples The following example shows how to clear the DF bit on all interfaces:

```
crypto ipsec df-bit clear
```

crypto ipsec df-bit (interface)

To set the DF bit for the encapsulating header in tunnel mode to a specific interface, use the **crypto ipsec df-bit** command in interface configuration mode.

crypto ipsec df-bit [**clear** | **set** | **copy**]

Syntax Description	clear	set	copy
	Outer IP header will have the DF bit cleared, and the router may fragment the packet to add the IP Security (IPSec) encapsulation.	Outer IP header will have the DF bit set; however, the router may fragment the packet if the original packet had the DF bit cleared.	The router will look in the original packet for the outer DF bit setting. The copy keyword is the default setting.

Defaults The default is **copy**.

Command Modes Interface configuration

Command History	Release	Modification
	12.2(2)T	This command was introduced.

Usage Guidelines Use the **crypto ipsec df-bit** command in interface configuration mode to configure your router to specify the DF bit in an encapsulated header. This command overrides any existing DF bit global settings.

You may want use the **clear** setting for the DF bit when encapsulating tunnel mode IPSec traffic so you can send packets larger than the available maximum transmission unit (MTU) size or if you do not know what the available MTU size is.

If this command is enabled without a specified setting, the router will use the **copy** setting as default.

Examples In following example, the router is configured to globally clear the setting for the DF bit and copy the DF bit on the interface named Ethernet0. Thus, all interfaces *except* Ethernet0 will allow the router to send packets larger than the available MTU size; Ethernet0 will allow the router to fragment the packet.

```
crypto isakmp policy 1
  hash md5
  authentication pre-share
crypto isakmp key Delaware address 192.168.10.66
crypto isakmp key Key-What-Key address 192.168.11.19
!
!
crypto ipsec transform-set BearMama ah-md5-hmac esp-des

crypto ipsec df-bit clear
!
!
```

```
crypto map armadillo 1 ipsec-isakmp
set peer 192.168.10.66
set transform-set BearMama
match address 101
!
crypto map basilisk 1 ipsec-isakmp
set peer 192.168.11.19
set transform-set BearMama
match address 102

!
!
interface Ethernet0
 ip address 192.168.10.38 255.255.255.0
 ip broadcast-address 0.0.0.0
 media-type 10BaseT
 crypto map armadillo
 crypto ipsec df-bit copy
!
interface Ethernet1
 ip address 192.168.11.75 255.255.255.0
 ip broadcast-address 0.0.0.0
 media-type 10BaseT
 crypto map basilisk
!
interface Serial0
 no ip address
 ip broadcast-address 0.0.0.0
 no ip route-cache
 no ip mroute-cache
```

crypto ipsec fragmentation (global)

To enable prefragmentation for IP Security (IPSec) Virtual Private Networks (VPNs) on a global basis, use the **crypto ipsec fragmentation** command in global configuration mode. To disable a manually configured command, use the **no** form of this command.

crypto ipsec fragmentation { **before-encryption** | **after-encryption** }

no crypto ipsec fragmentation { **before-encryption** | **after-encryption** }

Syntax Description

before-encryption	Enables prefragmentation for IPSec VPNs. The default is that prefragmentation is enabled.
after-encryption	Disables prefragmentation for IPSec VPNs.

Command Default

If you do not enter this command, prefragmentation is enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.1(11b)E	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Use the **before-encryption** keyword to enable prefragmentation for IPSec VPNs; use the **after-encryption** keyword to disable prefragmentation for IPSec VPNs. This command allows an encrypting router to predetermine the encapsulated packet size from information available in transform sets, which are configured as part of the IPSec security association (SA). If it is predetermined that the packet will exceed the maximum transmission unit (MTU) of the output interface, the packet is fragmented before encryption.



Note

This command does not show up in the a running configuration if the default global command is enabled. It shows in the running configuration only when you explicitly enable the command on an interface.

Examples

The following example shows how to globally enable prefragmentation for IPSec VPNs:

```
crypto ipsec fragmentation before-encryption
```

crypto ipsec fragmentation (interface)

To enable prefragmentation for IP Security (IPSec) Virtual Private Networks (VPNs) on an interface, use the **crypto ipsec fragmentation** command in interface configuration mode. To disable a manually configured command, use the **no** form of this command.

```
crypto ipsec fragmentation { before-encryption | after-encryption }
```

```
no crypto ipsec fragmentation { before-encryption | after-encryption }
```

Syntax Description

before-encryption	Enables prefragmentation for IPSec VPNs.
after-encryption	Disables prefragmentation for IPSec VPNs.

Defaults

If no other prefragmentation for IPSec VPNs commands are in the configuration, the router will revert to the default global configuration.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(11b)E	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines

Use the **before-encryption** keyword to enable prefragmentation for IPSec VPNs per interface; use the **after-encryption** keyword to disable prefragmentation for IPSec VPNs. This command allows an encrypting router to predetermine the encapsulated packet size from information available in transform sets, which are configured as part of the IPSec security association (SA). If it is predetermined that the packet will exceed the maximum transmission unit (MTU) of output interface, the packet is fragmented before encryption.

Examples

The following example shows how to enable prefragmentation for IPSec VPNs on an interface and then how to display the output of the show running configuration command:



Note

This command shows in the running configuration only when you explicitly enable it on the interface.

```
Router(config-if)# crypto ipsec fragmentation before-encryption
Router(config-if)# exit

Router# show running-config

crypto isakmp policy 10
 authentication pre-share
crypto isakmp key abcd123 address 209.165.202.130
!
```

```
crypto ipsec transform-set fooprime esp-3des esp-sha-hmac
!  
crypto map bar 10 ipsec-isakmp  
  set peer 209.165.202.130  
  set transform-set fooprime  
  match address 102
```

crypto ipsec nat-transparency

To enable security parameter index (SPI) matching or User Datagram Protocol (UDP) encapsulation between two Virtual Private Network (VPN) devices, use the **crypto ipsec nat-transparency** command on both devices in global configuration mode. To disable both SPI matching and UDP encapsulation, use the **no** form of this command with each keyword.

```
crypto ipsec nat-transparency {spi-matching | udp-encaps}
```

```
no crypto ipsec nat-transparency {spi-matching | udp-encaps}
```

Syntax Description	spi-matching	Enables SPI matching on both endpoints.
	udp-encaps	Enables UDP encapsulation on both endpoints.

Defaults When this command is entered, UDP encapsulation is enabled by default.

Command Modes Global configuration

Command History	Release	Modification
	12.2(13)T	This command was introduced.
	12.2(15)T	The command syntax was modified to add the spi-matching keyword.

Usage Guidelines You can use this command to resolve issues that arise when Network Address Translation (NAT) is configured in an IP Security (IPsec)-aware network. This command has two mutually exclusive options:

- The default option is UDP encapsulation of the IPsec protocols.
- The alternative is to match the inbound SPI to the outbound SPI.

When you enter the **crypto ipsec nat-transparency** command, UDP encapsulation is configured unless you either specifically disable it or configure SPI matching. You can disable both options, but doing so might cause problems if the device you are configuring uses NAT and is part of a VPN.

To disable SPI matching, configure UDP encapsulation or use the **no** form of this command with the keyword **spi-matching**. To disable UDP encapsulation, configure SPI matching or use the **no** form of this command with the keyword **udp-encaps**. To disable both SPI matching and UDP encapsulation, first disable UDP encapsulation, and then disable SPI matching. If you disable both options, the **show running-config** command displays: **no crypto ipsec nat-transparency udp-encaps**.

Examples The following example enables SPI matching on the endpoint routers:

```
crypto ipsec nat-transparency spi-matching
```

Related Commands

Command	Description
clear ip nat translation	Clears dynamic NAT translations from the translation table.
ip nat	Designates that traffic originating from or destined for the interface is subject to NAT.
ip nat inside destination	Enables NAT of the inside destination address.
ip nat inside source	Enables NAT of the inside source address.
ip nat outside source	Enables NAT of the outside source address.
show ip nat statistics	Displays NAT statistics.
show ip nat translations	Displays active NAT translations.
show crypto isakmp sa detail nat	Displays NAT translations of source and destination addresses.

crypto ipsec optional

To enable IP Security (IPSec) passive mode, use the **crypto ipsec optional** command in global configuration mode. To disable IPSec passive mode, use the **no** form of this command.

crypto ipsec optional

no crypto ipsec optional

Syntax Description This command has no arguments or keywords.

Defaults IPSec passive mode is not enabled.

Command Modes Global configuration

Command History	Release	Modification
	12.2(13)T	This command was introduced.

Usage Guidelines Use the **crypto ipsec optional** command to implement an intermediate mode (IPSec passive mode) that allows a router to accept unencrypted and encrypted data. IPSec passive mode is valuable for users who wish to migrate existing networks to IPSec because all routers will continue to interact with routers that encrypt data (that is, that have been upgraded with IPSec) and also with routers that have yet to be upgraded.

After this feature is disabled, all active connections that are sending unencrypted packets are cleared, and a message that reminds the user to enter the **write memory** command is sent.



Note

Because a router in IPSec passive mode is insecure, ensure that no routers are accidentally left in this mode after upgrading a network.

Examples The following example shows how to enable IPSec passive mode:

```
crypto map xauthmap 10 ipsec-isakmp
  set peer 209.165.202.145
  set transform-set xauthtransform
  match address 192
!
crypto ipsec optional
!
interface Ethernet1/0
  ip address 209.165.202.147 255.255.255.224
  crypto map xauthmap
!
access-list 192 permit ip host 209.165.202.147 host 209.165.202.145
```

crypto ipsec optional retry

To adjust the amount of time that a packet can be routed in the clear (unencrypted), use the **crypto ipsec optional retry** command in global configuration mode. To return to the default setting (5 minutes), use the **no** form of this command.

crypto ipsec optional retry *seconds*

no crypto ipsec optional retry *seconds*

Syntax Description	<i>seconds</i>	Time a connection can exist before another attempt is made to establish an encrypted IP Security (IPSec) session. The default value is 5 minutes.
---------------------------	----------------	---

Defaults	5 minutes
-----------------	-----------

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	12.2(13)T	This command was introduced.

Usage Guidelines	You must enable the crypto ipsec optional command, which enables IPSec passive mode, before you can use this command.
-------------------------	--

Examples The following example shows how to enable IPSec passive mode:

```
crypto map xauthmap 10 ipsec-isakmp
  set peer 209.165.202.145
  set transform-set xauthtransform
  match address 192
!
crypto ipsec optional
crypto ipsec optional retry 60
!
interface Ethernet1/0
 ip address 209.165.202.147 255.255.255.224
 crypto map xauthmap
!
access-list 192 permit ip host 209.165.202.147 host 209.165.202.145
```

Related Commands	Command	Description
	crypto ipsec optional	Enables IPSec passive mode.

crypto ipsec profile

To define the IPSECURITY (IPSec) parameters that are to be used for IPSec encryption between two IPSec routers, use the **crypto ipsec profile** command in global configuration mode. To delete an IPSec profile, use the **no** form of this command.

crypto ipsec profile *name*

no crypto ipsec profile *name*

Syntax Description	<i>name</i>	Profile name.
--------------------	-------------	---------------

Defaults An IPSec profile is not defined.

Command Modes Global configuration

Command History	Release	Modification
	12.2(13)T	This command was introduced.

Usage Guidelines An IPSec profile abstracts the IPSec policy settings into a single profile that can be used in other parts of the Cisco IOS configuration.

The IPSec profile shares most of the same commands with the crypto map configuration, but only a subset of the commands are valid in an IPSec profile. Only commands that pertain to an IPSec policy can be issued under an IPSec profile; you cannot specify the IPSec peer address or the access control list (ACL) to match the packets that are to be encrypted.

The following valid commands can be configured under an IPSec profile:

- **set-transform-set**—Specifies a list of transform sets in order of priority.
- **set pfs**—Specifies perfect forward secrecy (PFS) settings.
- **set security-association**—Defines security association parameters.
- **set-identity**—Specifies identity restrictions.

After enabling this command, the only parameter that *must* be defined under the profile is the transform set via the **set transform-set** command.

For more information on transform sets, refer to the section “Defining Transform Sets” in the chapter “Configuring IPSec Network Security” in the *Cisco IOS Security Configuration Guide*.

Examples

The following example shows how to configure a crypto map that uses an IPsec profile:

```
crypto ipsec transform-set cat-transforms esp-des esp-sha-hmac
 mode transport
!
crypto ipsec profile cat-profile
 set transform-set cat-transforms
 set pfs group2
!
crypto map foo 10 ipsec-isakmp
 set peer 10.13.7.67
 set profile foo-profile
 match address 101
```

Related Commands

Command	Description
crypto ipsec transform-set	Defines a transform set.
set pfs	Specifies that IP Security should ask for PFS when requesting new security associations for a crypto map entry.
set transform-set	Specifies which transform sets can be used with the crypto map entry.
tunnel protection	Associates a tunnel interface with an IPsec profile.

crypto ipsec security-association idle-time

To configure the IP Security (IPSec) security association (SA) idle timer, use the **crypto ipsec security-association idle-time** command in global configuration mode or crypto map configuration mode. To inactivate the IPSec SA idle timer, use the **no** form of this command.

crypto ipsec security-association idle-time *seconds*

no crypto ipsec security-association idle-time

Syntax Description	<i>seconds</i>	Time, in seconds, that the idle timer will allow an inactive peer to maintain an SA. Valid values for the <i>seconds</i> argument range from 60 to 86400.
---------------------------	----------------	---

Defaults	IPSec SA idle timers are disabled.
-----------------	------------------------------------

Command Modes	Global configuration Crypto map configuration
----------------------	--

Command History	Release	Modification
	12.2(15)T	This command was introduced.

Usage Guidelines	<p>Use the crypto ipsec security-association idle-time command to configure the IPSec SA idle timer. This timer controls the amount of time that an SA will be maintained for an idle peer.</p> <p>Use the crypto ipsec security-association lifetime command to configure global lifetimes for IPSec SAs. There are two lifetimes: a “timed” lifetime and a “traffic-volume” lifetime. A security association expires after the first of these lifetimes is reached.</p> <p>The IPSec SA idle timers are different from the global lifetimes for IPSec SAs. The expiration of the global lifetimes is independent of peer activity. The IPSec SA idle timer allows SAs associated with inactive peers to be deleted before the global lifetime has expired.</p> <p>If the IPSec SA idle timers are not configured with the crypto ipsec security-association idle-time command, only the global lifetimes for IPSec SAs are applied. SAs are maintained until the global timers expire, regardless of peer activity.</p>
-------------------------	--



Note	If the last IPSec SA to a given peer is deleted due to idle timer expiration, the Internet Key Exchange (IKE) SA to that peer will also be deleted.
-------------	---

Examples	The following example configures the IPSec SA idle timer to drop SAs for inactive peers after 600 seconds:
-----------------	--

```
crypto ipsec security-association idle-time 600
```

Related Commands

Command	Description
clear crypto sa	Deletes IPsec SAs.
crypto ipsec security-association lifetime	Changes global lifetime values used when negotiating IPsec SAs.

crypto ipsec security-association lifetime

To change global lifetime values used when negotiating IPsec security associations, use the **crypto ipsec security-association lifetime** command in global configuration mode. To reset a lifetime to the default value, use the **no** form of this command.

```
crypto ipsec security-association lifetime {seconds seconds | kilobytes kilobytes}
```

```
no crypto ipsec security-association lifetime {seconds | kilobytes}
```

Syntax Description	seconds <i>seconds</i>	<i>kilobytes</i> <i>kilobytes</i>
	Specifies the number of seconds a security association will live before expiring. The default is 3600 seconds (one hour).	Specifies the volume of traffic (in kilobytes) that can pass between IPsec peers using a given security association before that security association expires. The default is 4,608,000 kilobytes.

Defaults 3600 seconds (one hour) and 4,608,000 kilobytes (10 megabits per second for one hour).

Command Modes Global configuration

Command History	Release	Modification
	11.3 T	This command was introduced.

Usage Guidelines IPsec security associations use shared secret keys. These keys and their security associations time out together.

Assuming that the particular crypto map entry does not have lifetime values configured, when the router requests new security associations during security association negotiation, it will specify its global lifetime value in the request to the peer; it will use this value as the lifetime of the new security associations. When the router receives a negotiation request from the peer, it will use the smaller of the lifetime value proposed by the peer or the locally configured lifetime value as the lifetime of the new security associations.

There are two lifetimes: a “timed” lifetime and a “traffic-volume” lifetime. The security association expires after the first of these lifetimes is reached.

If you change a global lifetime, the change is only applied when the crypto map entry does not have a lifetime value specified. The change will not be applied to existing security associations, but will be used in subsequent negotiations to establish new security associations. If you want the new settings to take effect sooner, you can clear all or part of the security association database by using the **clear crypto sa** command. Refer to the **clear crypto sa** command for more details.

To change the global timed lifetime, use the **crypto ipsec security-association lifetime seconds** form of the command. The timed lifetime causes the security association to time out after the specified number of seconds have passed.

To change the global traffic-volume lifetime, use the **crypto ipsec security-association lifetime kilobytes** form of the command. The traffic-volume lifetime causes the security association to time out after the specified amount of traffic (in kilobytes) has been protected by the security associations' key.

Shorter lifetimes can make it harder to mount a successful key recovery attack, since the attacker has less data encrypted under the same key to work with. However, shorter lifetimes require more CPU processing time for establishing new security associations.

The lifetime values are ignored for manually established security associations (security associations installed using an **ipsec-manual** crypto map entry).

How These Lifetimes Work

The security association (and corresponding keys) will expire according to whichever occurs sooner, either after the number of seconds has passed (specified by the **seconds** keyword) or after the amount of traffic in kilobytes has passed (specified by the **kilobytes** keyword).

A new security association is negotiated *before* the lifetime threshold of the existing security association is reached, to ensure that a new security association is ready for use when the old one expires. The new security association is negotiated either 30 seconds before the **seconds** lifetime expires or when the volume of traffic through the tunnel reaches 256 kilobytes less than the **kilobytes** lifetime (whichever occurs first).

If no traffic has passed through the tunnel during the entire life of the security association, a new security association is not negotiated when the lifetime expires. Instead, a new security association will be negotiated only when IPSec sees another packet that should be protected.

Examples

The following example shortens both lifetimes, because the administrator feels there is a higher risk that the keys could be compromised. The timed lifetime is shortened to 2700 seconds (45 minutes), and the traffic-volume lifetime is shortened to 2,304,000 kilobytes (10 megabits per second for one half hour).

```
crypto ipsec security-association lifetime seconds 2700
crypto ipsec security-association lifetime kilobytes 2304000
```

Related Commands

Command	Description
set security-association lifetime	Overrides (for a particular crypto map entry) the global lifetime value, which is used when negotiating IPSec security associations.
show crypto ipsec security-association lifetime	Displays the security-association lifetime value configured for a particular crypto map entry.

crypto ipsec transform-set

To define a transform set—an acceptable combination of security protocols and algorithms—use the **crypto ipsec transform-set** command in global configuration mode. To delete a transform set, use the **no** form of this command.

```
crypto ipsec transform-set transform-set-name transform1 [transform2] [transform3]
[transform4]
```

```
no crypto ipsec transform-set transform-set-name
```

Syntax Description	
<i>transform-set-name</i>	Name of the transform set to create (or modify).
<i>transform1</i>	Type of transform. You may specify up to four “transforms”: one Authentication Header (AH), one Encapsulating Security Payload (ESP) encryption, one ESP authentication, and one compression. These transforms define the IP Security (IPSec) security protocols and algorithms. Accepted transform values are described in Table 11 .
<i>transform2</i>	
<i>transform3</i>	
<i>transform4</i>	

Defaults No default behavior or values

Command Modes Global configuration.
This command invokes the crypto transform configuration mode.

Command History	Release	Modification
	11.3 T	This command was introduced.
	12.2(13)T	The following transform options were added: esp-aes , esp-aes 192 , and esp-aes 256 .

Usage Guidelines A transform set is an acceptable combination of security protocols, algorithms, and other settings to apply to IPSec protected traffic. During the IPSec security association (SA) negotiation, the peers agree to use a particular transform set when protecting a particular data flow.

You can configure multiple transform sets, and then specify one or more of these transform sets in a crypto map entry. The transform set defined in the crypto map entry is used in the IPSec SA negotiation to protect the data flows specified by that crypto map entry’s access list. During the negotiation, the peers search for a transform set that is the same at both peers. When such a transform set is found, it is selected and will be applied to the protected traffic as part of both peer’s IPSec SAs.

When Internet Key Exchange (IKE) is not used to establish SAs, a single transform set must be used. The transform set is not negotiated.

Before a transform set can be included in a crypto map entry it must be defined using this command.

A transform set specifies one or two IPSec security protocols (either AH, ESP, or both) and specifies which algorithms to use with the selected security protocol. The AH and ESP IPSec security protocols are described in the section “[IPSec Protocols: AH and ESP](#).”

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

In a transform set you could specify the AH protocol, the ESP protocol, or both. If you specify an ESP protocol in a transform set, you can specify just an ESP encryption transform or both an ESP encryption transform and an ESP authentication transform.

[Table 11](#) lists the acceptable transform combination selections for the AH and ESP protocols.

Table 11 Allowed Transform Combinations

Transform Type	Transform	Description
AH Transform (<i>Pick only one.</i>)	ah-md5-hmac	AH with the MD5 (Message Digest 5) (a Hash-based Message Authentication Code [HMAC] variant) authentication algorithm
	ah-sha-hmac	AH with the SHA (Secure Hash Algorithm) (an HMAC variant) authentication algorithm
ESP Encryption Transform (<i>Pick only one.</i>)	esp-aes	ESP with the 128-bit Advanced Encryption Standard (AES) encryption algorithm
	esp-aes 192	ESP with the 192-bit AES encryption algorithm
	esp-aes 256	ESP with the 256-bit AES encryption algorithm
	esp-des	ESP with the 56-bit Data Encryption Standard (DES) encryption algorithm
	esp-3des	ESP with the 168-bit DES encryption algorithm (3DES or Triple DES)
	esp-null	Null encryption algorithm
ESP Authentication Transform (<i>Pick only one.</i>)	esp-md5-hmac	ESP with the MD5 (HMAC variant) authentication algorithm
	esp-sha-hmac	ESP with the SHA (HMAC variant) authentication algorithm
IP Compression Transform	comp-lzs	IP compression with the Lempel-Ziv-Stac (LZS) algorithm

Examples of acceptable transform combinations are as follows:

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

The parser will prevent you from entering invalid combinations; for example, once you specify an AH transform it will not allow you to specify another AH transform for the current transform set.

IPSec Protocols: AH and ESP

Both the AH and ESP protocols implement security services for IPSec.

AH provides data authentication and antireplay services.

ESP provides packet encryption and optional data authentication and antireplay services.

ESP encapsulates the protected data—either a full IP datagram (or only the payload)—with an ESP header and an ESP trailer. AH is embedded in the protected data; it inserts an AH header immediately after the outer IP header and before the inner IP datagram or payload. Traffic that originates and terminates at the IPSec peers can be sent in either tunnel or transport mode; all other traffic is sent in tunnel mode. Tunnel mode encapsulates and protects a full IP datagram, while transport mode encapsulates/protects the payload of an IP datagram. For more information about modes, see the **mode** (IPSec) command description.

Selecting Appropriate Transforms

The following tips may help you select transforms that are appropriate for your situation:

- If you want to provide data confidentiality, include an ESP encryption transform.
- If you want to ensure data authentication for the outer IP header as well as the data, include an AH transform. (Some consider the benefits of outer IP header data integrity to be debatable.)
- If you use an ESP encryption transform, also consider including an ESP authentication transform or an AH transform to provide authentication services for the transform set.
- If you want data authentication (either using ESP or AH), you can choose from the MD5 or SHA (HMAC keyed hash variants) authentication algorithms. The SHA algorithm is generally considered stronger than MD5 but is slower.
- Note that some transforms might not be supported by the IPSec peer.



Note If a user enters an IPSec transform that the hardware (the IPSec peer) does not support, a warning message will be displayed immediately after the **crypto ipsec transform-set** command is entered.

- In cases where you need to specify an encryption transform but do not actually encrypt packets, you can use the **esp-null** transform.

Suggested transform combinations follow:

- **esp-des** and **esp-sha-hmac**
- **ah-sha-hmac** and **esp-des** and **esp-sha-hmac**

The Crypto Transform Configuration Mode

After you issue the **crypto ipsec transform-set** command, you are put into the crypto transform configuration mode. While in this mode, you can change the mode to tunnel or transport. (These are optional changes.) After you have made these changes, type **exit** to return to global configuration mode. For more information about these optional changes, see the **match address** (IPSec) and **mode** (IPSec) command descriptions.

Changing Existing Transforms

If one or more transforms are specified in the **crypto ipsec transform-set** command for an existing transform set, the specified transforms will replace the existing transforms for that transform set.

If you change a transform set definition, the change is only applied to crypto map entries that reference the transform set. The change will not be applied to existing SAs, but will be used in subsequent negotiations to establish new SAs. If you want the new settings to take effect sooner, you can clear all or part of the SA database by using the **clear crypto sa** command.

Examples

The following example defines two transform sets. The first transform set will be used with an IPSec peer that supports the newer ESP and AH protocols. The second transform set will be used with an IPSec peer that only supports the older transforms.

```
crypto ipsec transform-set newer esp-3des esp-sha-hmac
crypto ipsec transform-set older ah-rfc-1828 esp-rfc1829
```

The following example is a sample warning message that is displayed when a user enters an IPSec transform that the hardware does not support:

```
crypto ipsec transform transform-1 esp-aes 256 esp-md5
WARNING:encryption hardware does not support transform
esp-aes 256 within IPSec transform transform-1
```

Related Commands

Command	Description
clear crypto sa	Deletes IPSec security associations.
crypto ipsec transform-set	Defines a transform set—an acceptable combination of security protocols and algorithms.
match address	Specifies an extended access list for a crypto map entry.
mode (IPSec)	Changes the mode for a transform set.
set transform-set	Specifies which transform sets can be used with the crypto map entry.
show crypto ipsec transform-set	Displays the configured transform sets.

crypto isakmp aggressive-mode disable

To block all Internet Security Association and Key Management Protocol (ISAKMP) aggressive mode requests to and from a device, use the **crypto isakmp aggressive-mode disable** command in global configuration mode. To disable the blocking, use the **no** form of this command.

crypto isakmp aggressive-mode disable

no crypto isakmp aggressive-mode disable

Syntax Description

This command has no arguments or keywords.

Defaults

If this command is not configured, Cisco IOS software will attempt to process all incoming ISAKMP aggressive mode security association (SA) connections. In addition, if the device has been configured with the **crypto isakmp peer address** and the **set aggressive-mode password** or **set aggressive-mode client-endpoint** commands, the device will initiate aggressive mode if this command is not configured.

Command Modes

Global configuration

Command History

Release	Modification
12.3(1)	This command was introduced on all Cisco IOS platforms that support IP Security (IPSec).

Usage Guidelines

If you configure this command, all aggressive mode requests to the device and all aggressive mode requests made by the device are blocked, regardless of the ISAKMP authentication type (preshared keys or Rivest, Shamir, and Adelman [RSA] signatures).

If a request is made by or to the device for aggressive mode, the following syslog notification is sent:

```
Unable to initiate or respond to Aggressive Mode while disabled
```



Note

This command will prevent Easy Virtual Private Network (Easy VPN) clients from connecting if they are using preshared keys because Easy VPN clients (hardware and software) use aggressive mode.

Examples

The following example shows that all aggressive mode requests to and from a device are blocked:

```
Router (config)# crypto isakmp aggressive-mode disable
```

crypto isakmp client configuration address-pool local

To configure the IP address local pool to reference Internet Key Exchange (IKE) on your router, use the **crypto isakmp client configuration address-pool local** command in global configuration mode. To restore the default value, use the **no** form of this command.

crypto isakmp client configuration address-pool local *pool-name*

no crypto isakmp client configuration address-pool local

Syntax Description	<i>pool-name</i>	Specifies the name of a local address pool.
---------------------------	------------------	---

Defaults	IP address local pools do not reference IKE.
-----------------	--

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	12.0(4)XE	This command was introduced.
	12.0(7)T	This command was integrated into Cisco IOS release 12.0(7)T.

Examples	The following example references IP address local pools to IKE on your router, with “ire” as the <i>pool-name</i> :
-----------------	---

```
crypto isakmp client configuration address-pool local ire
```

Related Commands	Command	Description
	ip local pool	Configures a local pool of IP addresses to be used when a remote peer connects to a point-to-point interface.

crypto isakmp client configuration group

To specify which group's policy profile will be defined, use the **crypto isakmp client configuration group** command in global configuration mode. To remove this command and all associated subcommands from your configuration, use the **no** form of this command.

crypto isakmp client configuration group { *group-name* | **default** }

no crypto isakmp client configuration group { *group-name* | **default** }

Syntax Description

<i>group-name</i>	Group definition that identifies which policy is enforced for users.
default	Policy that is enforced for all users who do not offer a group name that matches a <i>group-name</i> argument. The default keyword can only be configured locally.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.

Usage Guidelines

Use the **crypto isakmp client configuration group** command to specify group policy information that needs to be defined or changed. You may change the group policy on your router if you decide to connect to the client using a group identification that does not match the *group-name* argument.

After enabling this command, which puts you in Internet Security Association Key Management Protocol (ISAKMP) group configuration mode, you can specify characteristics for the group policy using the following commands:

- **acl**—Specifies a group of access control lists (ACLs) that represent protected subnets for split tunneling purposes.
- **dns**—Specifies the primary and secondary Domain Name Service (DNS) servers for the group.
- **domain (isakmp-group)**—Specifies group domain membership.
- **key (isakmp-group)**—Specifies the Internet Key Exchange (IKE) preshared key when defining group policy information for Mode Configuration push.
- **pool (isakmp-group)**—Refers to the IP local pool address used to allocate internal IP addresses to clients.
- **wins**—Specifies the primary and secondary Windows Internet Naming Service (WINS) servers for the group.

Examples

The following example shows how to define group policy information for Mode Configuration push. In this example, the first group name is “cisco” and the second group name is “default.” Thus, the default policy will be enforced for all users who do not offer a group name that matches “cisco.”

```
crypto isakmp client configuration group cisco
  key cisco
  dns 2.2.2.2 2.2.2.3
  wins 6.6.6.6
  domain cisco.com
  pool fred
  acl 199
!
crypto isakmp client configuration group default
  key cisco
  dns 2.2.2.2 2.3.2.3
  pool fred
  acl 199
```

Related Commands

Command	Description
acl	Configures split tunneling.
dns	Specifies the primary and secondary DNS servers.
domain (isakmp-group)	Specifies the DNS domain to which a group belongs.
key (isakmp-group)	Specifies the IKE preshared key for group policy attribute definition.
pool (isakmp-group)	Defines a local pool address.
set aggressive-mode client-endpoint	Specifies the Tunnel-Client-Endpoint attribute within an ISAKMP peer configuration.

crypto isakmp enable

To globally enable Internet Key Exchange (IKE) at your peer router, use the **crypto isakmp enable** command in global configuration mode. To disable IKE at the peer, use the **no** form of this command.

crypto isakmp enable

no crypto isakmp enable

Syntax Description This command has no arguments or keywords.

Defaults IKE is enabled.

Command Modes Global configuration

Command History	Release	Modification
	11.3 T	This command was introduced.

Usage Guidelines IKE is enabled by default. IKE does not have to be enabled for individual interfaces, but is enabled globally for all interfaces at the router.

If you do not want IKE to be used in your IPSec implementation, you can disable IKE at all your IP Security peers. If you disable IKE at one peer, you must disable it at all your IPSec peers.

If you disable IKE, you will have to make these concessions at the peers:

- You must manually specify all the IPSec security associations (SAs) in the crypto maps at the peers. (Crypto map configuration is described in the chapter “Configuring IPSec Network Security” in the *Cisco IOS Security Configuration Guide*.)
- The IPSec SAs of the peers will never time out for a given IPSec session.
- During IPSec sessions between the peers, the encryption keys will never change.
- Anti-replay services will not be available between the peers.
- Certification authority (CA) support cannot be used.

Examples The following example disables IKE at one peer. (The same command should be issued at all remote peers.)

```
no crypto isakmp enable
```

crypto isakmp identity

To define the identity used by the router when participating in the Internet Key Exchange (IKE) protocol, use the **crypto isakmp identity** command in global configuration mode. Set an Internet Security Association Key Management Protocol (ISAKMP) identity whenever you specify preshared keys. To reset the ISAKMP identity to the default value (address), use the **no** form of this command.

crypto isakmp identity {address | hostname}

no crypto isakmp identity

Syntax Description	address	Sets the ISAKMP identity to the IP address of the interface that is used to communicate to the remote peer during IKE negotiations.
	hostname	Sets the ISAKMP identity to the host name concatenated with the domain name (for example, myhost.example.com).

Defaults The IP address is used for the ISAKMP identity.

Command Modes Global configuration

Command History	Release	Modification
	11.3 T	This command was introduced.

Usage Guidelines

Use this command to specify an ISAKMP identity either by IP address or by host name.

The **address** keyword is typically used when there is only one interface (and therefore only one IP address) that will be used by the peer for IKE negotiations, and the IP address is known.

The **hostname** keyword should be used if there is more than one interface on the peer that might be used for IKE negotiations, or if the interface's IP address is unknown (such as with dynamically assigned IP addresses).

As a general rule, you should set all peers' identities in the same way, either by IP address or by host name.

Examples The following example uses preshared keys at two peers and sets both their ISAKMP identities to IP address.

At the local peer (at 10.0.0.1) the ISAKMP identity is set and the preshared key is specified.

```
crypto isakmp identity address
crypto isakmp key sharedkeystring address 192.168.1.33
```

At the remote peer (at 192.168.1.33) the ISAKMP identity is set and the same preshared key is specified.

```
crypto isakmp identity address
crypto isakmp key sharedkeystring address 10.0.0.1
```

**Note**

In the preceding example if the **crypto isakmp identity** command had not been performed, the ISAKMP identities would have still been set to IP address, the default identity.

The following example uses preshared keys at two peers and sets both their ISAKMP identities to host name.

At the local peer the ISAKMP identity is set and the preshared key is specified.

```
crypto isakmp identity hostname
crypto isakmp key sharedkeystring hostname RemoteRouter.example.com
ip host RemoteRouter.example.com 192.168.0.1
```

At the remote peer the ISAKMP identity is set and the same preshared key is specified.

```
crypto isakmp identity hostname
crypto isakmp key sharedkeystring hostname LocalRouter.example.com
ip host LocalRouter.example.com 10.0.0.1 10.0.0.2
```

In the above example, host names are used for the peers' identities because the local peer has two interfaces that might be used during an IKE negotiation.

In the above example the IP addresses are also mapped to the host names; this mapping is not necessary if the routers' host names are already mapped in DNS.

Related Commands

Command	Description
crypto ipsec security-association lifetime	Specifies the authentication method within an IKE policy.
crypto isakmp key	Configures a preshared authentication key.

crypto isakmp keepalive

To allow the gateway to send dead peer detection (DPD) messages to the peer, use the **crypto isakmp keepalive** command in global configuration mode. To disable keepalives, use the **no** form of this command.

crypto isakmp keepalive *secs* [*retries*]

no crypto isakmp keepalive *secs* [*retries*]

Syntax Description	<i>seconds</i>	Number of seconds between DPD messages; the range is from 10 to 3600 seconds.
		Note If you do not specify a time interval, you will receive an error message.
	<i>retries</i>	(Optional) Number of seconds between DPD retries if the DPD message fails; the range is from 2 to 60 seconds. If unspecified, the default is 2 seconds.

Defaults No DPD messages are sent.

Command Modes Global configuration

Command History	Release	Modification
	12.2(8)T	This command was introduced.

Usage Guidelines Use the **crypto isakmp keepalive** command to enable the gateway to send DPD messages to the peer. DPD is a keepalives scheme that allows the router to query the liveliness of its Internet Key Exchange (IKE) peer.



Note When the **crypto isakmp keepalive** command is configured, the Cisco IOS software negotiates the use of Cisco IOS keepalives or DPD, depending on which protocol the peer supports.

Examples The following example shows how to configure DPD messages to be sent every 60 seconds and every 5 seconds between retries if the peer does not respond:

```
crypto isakmp keepalive 60 5
```

crypto isakmp key

To configure a preshared authentication key, use the **crypto isakmp key** command in global configuration mode. To delete a preshared authentication key, use the **no** form of this command.

crypto isakmp key *key-string* **address** *peer-address* [*mask*] [**no-xauth**]

no crypto isakmp key *key-string* **address** *peer-address*

Syntax Description		
<i>key-string</i>	Specifies the preshared key. Use any combination of alphanumeric characters up to 128 bytes. This preshared key must be identical at both peers.	
address	Use this keyword if the remote peer Internet Security Association Key Management Protocol (ISAKMP) identity was set with its IP address.	
<i>peer-address</i>	Specifies the IP address of the remote peer.	
<i>mask</i>	(Optional) Specifies the subnet address of the remote peer. (The argument can be used only if the remote peer ISAKMP identity was set with its IP address.)	
no-xauth	(Optional) Use this keyword if router-to-router IP Security (IPSec) is on the same crypto map as a Virtual Private Network (VPN)-client-to-Cisco IOS IPSec. This keyword prevents the router from prompting the peer for extended authentication (Xauth) information (username and password).	

Defaults There is no default preshared authentication key.

Command Modes Global configuration

Command History	Release	Modification
	11.3 T	This command was introduced.
	12.1(1)T	The <i>mask</i> argument was added.
	12.2(4)T	The no-xauth keyword was added.

Usage Guidelines You must use this command to configure a key whenever you specify preshared keys in an Internet Key Exchange (IKE) policy; you must enable this command at both peers.

If an IKE policy includes preshared keys as the authentication method, these preshared keys must be configured at both peers—otherwise the policy cannot be used (the policy will not be submitted for matching by the IKE process). The **crypto isakmp key** command is the second task required to configure the preshared keys at the peers. (The first task is accomplished using the **crypto isakmp identity** command.)

Use the **address** keyword if the remote peer ISAKMP identity was set with its IP address.

With the **address** keyword, you can also use the *mask* argument to indicate the remote peer ISAKMP identity will be established using the preshared key only. If the *mask* argument is used, preshared keys are no longer restricted between two users.

**Note**

If you specify *mask*, you must use a subnet address. (The subnet address 0.0.0.0 is not recommended because it encourages group preshared keys, which allow all peers to have the same group key, thereby reducing the security of your user authentication.)

Preshared keys no longer work when the hostname keyword is sent as the identity; thus, the hostname keyword as the identity in preshared key authentication is no longer supported. According to the way preshared key authentication is designed in IKE main mode, the preshared keys *must* be based on the IP address of the peers. Although a user can still send the hostname as identity in preshared key authentication, the key is searched on the IP address of the peer; if the key is not found (based on the IP address), the negotiation will fail.

If **crypto isakmp identity hostname** is configured as identity, the preshared key *must* be configured with the peer's IP address for the process to work.

Use the **no-xauth** keyword to prevent the router from prompting the peer for Xauth information (username and password). This keyword disables Xauth for static IPsec peers. The **no-xauth** keyword should be enabled when configuring the preshared key for router-to-router IPsec—not VPN-client-to-Cisco IOS IPsec.

Examples

In the following example, the remote peer “RemoteRouter” specifies an ISAKMP identity by address:

```
crypto isakmp identity address
```

Now, the preshared key must be specified at each peer.

In the following example, the local peer specifies the preshared key and designates the remote peer by its IP address and a mask:

```
crypto isakmp key sharedkeystring address 172.21.230.33 255.255.255.255
```

Related Commands

Command	Description
crypto ipsec security-association lifetime	Specifies the authentication method within an IKE policy.
crypto isakmp identity	Defines the identity the router uses when participating in the IKE protocol.
ip host	Defines a static host name-to-address mapping in the host cache.

crypto isakmp nat keepalive

To allow an IP Security (IPSec) node to send Network Address Translation (NAT) keepalive packets, use the **crypto isakmp nat keepalive** command in global configuration mode. To disable NAT keepalive packets, use the **no** form of this command.

crypto isakmp nat keepalive *seconds*

no crypto isakmp nat keepalive

Syntax Description	<i>seconds</i>	Number of seconds between keepalive packets; the range is between 5 and 3600 seconds.
---------------------------	----------------	---

Defaults	NAT keepalive packets are not sent.
-----------------	-------------------------------------

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	12.2(13)T	This command was introduced.

Usage Guidelines The **crypto isakmp nat keepalive** command allows users to keep the dynamic NAT mapping alive during a connection between two peers. A NAT keepalive beat is sent if IPSec does not send or receive a packet within a specified time period.

If this command is enabled, users should ensure that the idle value is shorter than the NAT mapping expiration time.

Examples The following example shows how to enable NAT keepalives to be sent every 20 seconds:

```
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key 1234 address 209.165.202.130
crypto isakmp nat keepalive 20
!
crypto ipsec transform-set t2 esp-des esp-sha-hmac
no crypto engine accelerator
!
crypto map test2 10 ipsec-isakmp
 set peer 209.165.202.130
 set transform-set t2
 match address 101
```

crypto isakmp peer

To enable an IP Security (IPSec) peer for Internet Key Exchange (IKE) querying of authentication, authorization, and accounting (AAA) for tunnel attributes in aggressive mode, use the **crypto isakmp peer** command in global configuration mode. To disable this functionality, use the **no** form of this command.

```
crypto isakmp peer {ip-address ip-address | fqdn fqdn} {vrf fvrf-name}
```

```
no crypto isakmp peer {ip-address ip-address | fqdn fqdn} {vrf fvrf-name}
```

Syntax Description		
ip-address <i>ip-address</i>	IP address of the peer router.	
fqdn <i>fqdn</i>	Fully qualified domain name (FQDN) of the peer router.	
vrf <i>fvrf-name</i>	Virtual routing and forwarding (VRF) routing table through which the peer is reachable.	

Defaults No default behavior or values

Command Modes Global configuration

Command History	Release	Modification
	12.2(8)T	This command was introduced.
	12.2(15)T	The vrf keyword and <i>fvrf-name</i> argument were added.

Usage Guidelines After enabling this command, you can use the **set aggressive-mode client-endpoint** and **set aggressive-mode password** commands to specify RADIUS tunnel attributes in the Internet Security Association and Key Management Protocol (ISAKMP) peer policy for IPSec peers.

Instead of keeping your preshared keys on the hub router, you can scale your preshared keys by storing and retrieving them from an AAA server. The preshared keys are stored in the AAA server as Internet Engineering Task Force (IETF) RADIUS tunnel attributes and are retrieved when a user tries to “speak” to the hub router. The hub router retrieves the preshared key from the AAA server and the spokes (the users) initiate aggressive mode to the hub by using the preshared key that is specified in the ISAKMP peer policy as a RADIUS tunnel attribute.

Examples The following example shows how to initiate aggressive mode using RADIUS tunnel attributes:

```
crypto isakmp peer ip-address 209.165.200.230 vrf vpn1
  set aggressive-mode client-endpoint user-fqdn user@cisco.com
  set aggressive-mode password cisco123
```

Related Commands	Command	Description
	crypto map isakmp authorization list	Enables IKE querying of AAA for tunnel attributes in aggressive mode.
	set aggressive-mode client-endpoint	Specifies the Tunnel-Client-Endpoint attribute within an ISAKMP peer configuration.
	set aggressive-mode password	Specifies the Tunnel-Password attribute within an ISAKMP peer configuration.

crypto isakmp policy

To define an Internet Key Exchange (IKE) policy, use the **crypto isakmp policy** command in global configuration mode. IKE policies define a set of parameters to be used during the IKE negotiation. To delete an IKE policy, use the **no** form of this command.

crypto isakmp policy *priority*

no crypto isakmp policy

Syntax Description	<i>priority</i> Uniquely identifies the IKE policy and assigns a priority to the policy. Use an integer from 1 to 10,000, with 1 being the highest priority and 10,000 the lowest.				
Defaults	If you do not configure any IKE policies, your router will use the default policy, which is always set to the lowest priority and which contains the default value of each parameter.				
Command Modes	Global configuration				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>11.3 T</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	11.3 T	This command was introduced.
Release	Modification				
11.3 T	This command was introduced.				
Usage Guidelines	<p>Use this command to specify the parameters to be used during an IKE negotiation. (These parameters are used to create the IKE security association [SA].)</p> <p>This command invokes the Internet Security Association Key Management Protocol (ISAKMP) policy configuration (config-isakmp) command mode. While in the ISAKMP policy configuration command mode, some of the commands for which you can specify parameters are as follows:</p> <ul style="list-style-type: none"> • encryption (IKE policy); default = 56-bit DES-CBC • hash (IKE policy); default = SHA-1 • authenticaion; default = RSA signatures • group (IKE policy); default = 768-bit Diffie-Hellman • lifetime (IKE policy); default = 86,400 seconds (one day) <p>If you do not specify any given parameter, the default value will be used for that parameter.</p> <p>To exit the config-isakmp command mode, type exit.</p> <p>You can configure multiple IKE policies on each peer participating in IPSec. When the IKE negotiation begins, it tries to find a common policy configured on both peers, starting with the highest priority policies as specified on the remote peer.</p>				

Examples

The following example configures two policies for the peer:

```
crypto isakmp policy 15
  hash md5
  authentication rsa-sig
  group 2
  lifetime 5000
crypto isakmp policy 20
  authentication pre-share
  lifetime 10000
```

The above configuration results in the following policies:

```
Router# show crypto isakmp policy

Protection suite priority 15
  encryption algorithm:DES - Data Encryption Standard (56 bit keys)
  hash algorithm:Message Digest 5
  authentication method:Rivest-Shamir-Adleman Signature
  Diffie-Hellman Group:#2 (1024 bit)
  lifetime:5000 seconds, no volume limit
Protection suite priority 20
  encryption algorithm:DES - Data Encryption Standard (56 bit keys)
  hash algorithm:Secure Hash Standard
  authentication method:preshared Key
  Diffie-Hellman Group:#1 (768 bit)
  lifetime:10000 seconds, no volume limit
Default protection suite
  encryption algorithm:DES - Data Encryption Standard (56 bit keys)
  hash algorithm:Secure Hash Standard
  authentication method:Rivest-Shamir-Adleman Signature
  Diffie-Hellman Group:#1 (768 bit)
  lifetime:86400 seconds, no volume limit
```

Related Commands

Command	Description
encryption (IKE policy)	Specifies the encryption algorithm within an IKE policy.
group (IKE policy)	Specifies the Diffie-Hellman group identifier within an IKE policy.
hash (IKE policy)	Specifies the hash algorithm within an IKE policy.
lifetime (IKE policy)	Specifies the lifetime of an IKE SA.
show crypto isakmp policy	Displays the parameters for each IKE policy.

crypto isakmp profile

To define an Internet Security Association and Key Management Protocol (ISAKMP) profile and to audit IP Security (IPSec) user sessions, use the **crypto isakmp profile** command in global configuration mode. To delete a crypto ISAKMP profile, use the **no** form of this command.

```
crypto isakmp profile profile-name [accounting aaalist]
```

```
no crypto isakmp profile profile-name [accounting aaalist]
```

Syntax Description	<i>profile-name</i>	Name of the user profile. To associate a user profile with the RADIUS server, the user profile name must be identified.
	accounting <i>aaalist</i>	(Optional) Name of a client accounting list.

Defaults No default behaviors or values

Command Modes Global configuration

Command History	Release	Modification
	12.2(15)T	This command was introduced.

Usage Guidelines

Defining an ISAKMP Profile

An ISAKMP profile can be viewed as a repository of Phase 1 and Phase 1.5 commands for a set of peers. The Phase 1 configuration includes commands to configure such things as keepalive, identity matching, and the authorization list. The Phase 1.5 configuration includes commands to configure such things as extended authentication (Xauth) and mode configuration.

The peers are mapped to an ISAKMP profile when their identities are matched (as given in the identification [ID] payload of the Internet Key Exchange [IKE]) against the identities defined in the ISAKMP profile. To uniquely map to an ISAKMP profile, no two ISAKMP profiles should match the same identity. If the peer identity is matched in two ISAKMP profiles, the configuration is invalid. Also, there must be at least one **match identity** command defined in the ISAKMP profile for it to be complete.

Auditing IPSec User Sessions

Use this command to audit multiple user sessions that are terminating on the IPSec gateway.



Note

The **crypto isakmp profile** command and the **crypto map (global IPSec)** command are mutually exclusive. If a profile is present (the **crypto isakmp profile** command has been used), with no accounting configured but with the global command present (the **crypto isakmp profile** command without the **accounting** keyword), accounting will occur using the attributes in the global command.

Examples

The following example shows how to define an ISAKMP profile and match the peer identities:

```
crypto isakmp profile vpnprofile
match identity address 10.76.11.53
```

The following accounting example shows that an ISAKMP profile is configured:

```
aaa new-model
!
!
aaa authentication login cisco-client group radius
aaa authorization network cisco-client group radius
aaa accounting network acc start-stop broadcast group radius
aaa session-id common
!
crypto isakmp profile cisco
vrf cisco
match identity group cclient
client authentication list cisco-client
isakmp authorization list cisco-client
client configuration address respond
accounting acc
!
crypto dynamic-map dynamic 1
set transform-set aswan
set isakmp-profile cisco
reverse-route
!
!
radius-server host 172.1.1.4 auth-port 1645 acct-port 1646
radius-server key nsite
```

Related Commands

Command	Description
crypto map (global IPSec)	Enters crypto map configuration mode and creates or modifies a crypto map entry, creates a crypto profile that provides a template for configuration of dynamically created crypto maps, or configures a client accounting list.
debug crypto isakmp	Displays messages about IKE events.
match identity	Matches an identity from a peer in an ISAKMP profile.

crypto key generate rsa

To generate Rivest, Shamir, and Adelman (RSA) key pairs, use the **crypto key generate rsa** command in global configuration mode.

crypto key generate rsa [**general-keys** | **usage-keys** | **signature** | **encryption**] [**label** *key-label*] [**exportable**] [**modulus** *modulus-size*] [**storage** *devicename:*] [**on** *devicename:*]

Syntax Description	
general-keys	(Optional) Specifies that a general-purpose key pair will be generated, which is the default.
usage-keys	(Optional) Specifies that two RSA special-usage key pairs, one encryption pair and one signature pair, will be generated.
signature	(Optional) Specifies that the RSA public key generated will be a signature special usage key.
encryption	(Optional) Specifies that the RSA public key generated will be an encryption special usage key.
label <i>key-label</i>	(Optional) Name that is used for an RSA key pair when they are being exported. If a key label is not specified, the fully qualified domain name (FQDN) of the router is used.
exportable	(Optional) Specifies that the RSA key pair can be exported to another Cisco device, such as a router.
modulus <i>modulus-size</i>	(Optional) Specifies the IP size of the key modulus. By default, the modulus of a CA key is 1024 bits. The recommended modulus for a CA key is 2048 bits. The range of a CA key modulus is from 350 to 2048 bits. If you do not enter the modulus keyword and specify a key size, you will be prompted.
storage <i>devicename:</i>	(Optional) Specifies the key storage location. The name of the storage device is followed by a colon (:).
on <i>devicename:</i>	(Optional) Specifies that the RSA key pair will be created on the specified device, including a USB token, local disk, or NVRAM. The name of the device is followed by a colon (:). Keys created on a USB token have a maximum size of 1024 bits.

Command Default RSA key pairs do not exist.

Command Modes Global configuration

Command History	Release	Modification
	11.3	This command was introduced.
	12.2(8)T	The <i>key-label</i> argument was added.
	12.2(15)T	The exportable keyword was added.
	12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.

Release	Modification
12.4(4)T	The storage keyword and <i>devicename:</i> argument were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(11)T	The storage keyword and <i>devicename:</i> argument were implemented on the Cisco 7200VXR NPE-G2 platform. The signature , encryption and on keywords and <i>devicename:</i> argument were added.

Usage Guidelines

Use this command to generate RSA key pairs for your Cisco device (such as a router).

RSA keys are generated in pairs—one public RSA key and one private RSA key.

If your router already has RSA keys when you issue this command, you will be warned and prompted to replace the existing keys with new keys.



Note

Before issuing this command, ensure that your router has a hostname and IP domain name configured (with the **hostname** and **ip domain-name** commands). You will be unable to complete the **crypto key generate rsa** command without a hostname and IP domain name. (This situation is not true when you only generate a named key pair.)



Note

Secure Shell (SSH) may generate an additional RSA key pair if you generate a key pair on a router having no RSA keys. The additional key pair is used only by SSH and will have a name such as *{router_FQDN}.server*. For example, if a router name is “router1.cisco.com,” the key name is “router1.cisco.com.server.”

This command is not saved in the router configuration; however, the RSA keys generated by this command are saved in the private configuration in NVRAM (which is never displayed to the user or backed up to another device) the next time the configuration is written to NVRAM.



Note

If the configuration is not saved to NVRAM, the generated keys are lost on the next reload of the router.

There are two mutually exclusive types of RSA key pairs: special-usage keys and general-purpose keys. When you generate RSA key pairs, you will be prompted to select either special-usage keys or general-purpose keys.

Special-Usage Keys

If you generate special-usage keys, two pairs of RSA keys will be generated. One pair will be used with any Internet Key Exchange (IKE) policy that specifies RSA signatures as the authentication method, and the other pair will be used with any IKE policy that specifies RSA encrypted keys as the authentication method.

A certification authority (CA) is used only with IKE policies specifying RSA signatures, not with IKE policies specifying RSA-encrypted nonces. (However, you could specify more than one IKE policy and have RSA signatures specified in one policy and RSA-encrypted nonces in another policy.)

If you plan to have both types of RSA authentication methods in your IKE policies, you may prefer to generate special-usage keys. With special-usage keys, each key is not unnecessarily exposed. (Without special-usage keys, one key is used for both authentication methods, increasing the exposure of that key.)

General-Purpose Keys

If you generate general-purpose keys, only one pair of RSA keys will be generated. This pair will be used with IKE policies specifying either RSA signatures or RSA encrypted keys. Therefore, a general-purpose key pair might get used more frequently than a special-usage key pair.

Named Key Pairs

If you generate a named key pair using the *key-pair-label* argument, you must also specify the **usage-keys** keyword or the **general-keys** keyword. Named key pairs allow you to have multiple RSA key pairs, enabling the Cisco IOS software to maintain a different key pair for each identity certificate.

Modulus Length

When you generate RSA keys, you will be prompted to enter a modulus length. The longer the modulus, the stronger the security. However a longer modulus takes longer to generate (see [Table 12](#) for sample times) and takes longer to use.

Cisco IOS software does not support a modulus greater than 4096 bits. A length of less than 512 bits is normally not recommended. In certain situations, the shorter modulus may not function properly with IKE, so we recommend using a minimum modulus of 1024 bits.



Note

As of Cisco IOS Release 12.4(11)T, peer *public* RSA key modulus values up to 4096 bits are automatically supported.

The largest private RSA key modulus is 2048 bits. Therefore, the largest RSA private key a router may generate or import is 2048 bits.

The recommended modulus for a CA is 2048 bits; the recommended modulus for a client is 1024 bits.

Table 12 Sample Times by Modulus Length to Generate RSA Keys

Router	360 bits	512 bits	1024 bits	2048 bits (maximum)
Cisco 2500	11 seconds	20 seconds	4 minutes, 38 seconds	more than 1 hour
Cisco 4700	less than 1 second	1 second	4 seconds	50 seconds

Specifying a Storage Location for RSA Keys

When you issue the **crypto key generate rsa** command with the **storage devicename:** keyword and argument, the RSA keys will be stored on the specified device. This location will supersede any **crypto key storage** command settings.

Specifying a Device for RSA Key Generation

As of Cisco IOS Release 12.4(11)T and later releases, you may specify the device where RSA keys are generated. Devices supported include NVRAM, local disks, and USB tokens. If your router has a USB token configured and available, the USB token can be used as cryptographic device in addition to a storage device. Using a USB token as a cryptographic device allows RSA operations such as key generation, signing, and authentication of credentials to be performed on the token. The private key never leaves the USB token and is not exportable. The public key is exportable.

RSA keys may be generated on a configured and available USB token, by the use of the **on devicename:** keyword and argument. Keys that reside on a USB token are saved to persistent token storage when they are generated. The number of keys that can be generated on a USB token is limited by the space available. If you attempt to generate keys on a USB token and it is full you will receive the following message:

```
% Error in generating keys:no available resources
```

Key deletion will remove the keys stored on the token from persistent storage immediately. (Keys that do not reside on a token are saved to or deleted from non-token storage locations when the **write memory** or similar command is issued.)

For information on configuring a USB token, see “[Storing PKI Credentials](#)” chapter in the *Cisco IOS Security Configuration Guide*, Release 12.4T. For information on using on-token RSA credentials, see “[Configuring and Managing a Cisco IOS Certificate Server for PKI Deployment](#)” chapter in the *Cisco IOS Security Configuration Guide*, Release 12.4T.

Examples

The following example generates a general usage 1024-bit RSA key pair on a USB token with the label “ms2” with crypto engine debugging messages shown:

```
Router(config)# crypto key generate rsa on usbtoken0 label ms2 modulus 1024
The name for the keys will be: ms2
% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be on-token, non-exportable...
Jan 7 02:41:40.895: crypto_engine: Generate public/private keypair [OK]
Jan 7 02:44:09.623: crypto_engine: Create signature
Jan 7 02:44:10.467: crypto_engine: Verify signature
Jan 7 02:44:10.467: CryptoEngine0: CRYPTO_ISA_RSA_CREATE_PUBKEY(hw) (ipsec)
Jan 7 02:44:10.467: CryptoEngine0: CRYPTO_ISA_RSA_PUB_DECRYPT(hw) (ipsec)
```

Now, the on-token keys labeled “ms2” may be used for enrollment.

The following example generates special-usage RSA keys:

```
Router(config)# crypto key generate rsa usage-keys
The name for the keys will be: myrouter.example.com
```

```
Choose the size of the key modulus in the range of 360 to 2048 for your Signature Keys.
Choosing a key modulus greater than 512 may take a few minutes.
How many bits in the modulus[512]? <return>
Generating RSA keys.... [OK].
```

```
Choose the size of the key modulus in the range of 360 to 2048 for your Encryption Keys.
Choosing a key modulus greater than 512 may take a few minutes.
How many bits in the modulus[512]? <return>
Generating RSA keys.... [OK].
```

The following example generates general-purpose RSA keys:



Note

You cannot generate both special-usage and general-purpose keys; you can generate only one or the other.

```
Router(config)# crypto key generate rsa general-keys
The name for the keys will be: myrouter.example.com
```

Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes.
How many bits in the modulus[512]? **<return>**
Generating RSA keys.... [OK].

The following example generates the general purpose RSA key pair “exampleCAkeys”:

```
crypto key generate rsa general-keys exampleCAkeys
crypto ca trustpoint exampleCAkeys
  enroll url http://exampleCAkeys/certsrv/mscep/mscep.dll
  rsakeypair exampleCAkeys 1024 1024
```

The following example specifies the RSA key storage location of “usbtoken0:” for “tokenkey1”:

```
crypto key generate rsa general-keys label tokenkey1 storage usbtoken0:
```

Related Commands

Command	Description
crypto key storage	Sets the default storage location for RSA key pairs.
debug crypto engine	Displays debug messages about crypto engines.
hostname	Specifies or modifies the hostname for the network server.
ip domain-name	Defines a default domain name to complete unqualified hostnames (names without a dotted-decimal domain name).
show crypto key mypubkey rsa	Displays the RSA public keys of your router.
show crypto pki certificates	Displays information about your PKI certificate, certification authority, and any registration authority certificates.

crypto key pubkey-chain rsa

To enter public key configuration mode (so you can manually specify other devices' RSA public keys), use the **crypto key pubkey-chain rsa** command in global configuration mode.

crypto key pubkey-chain rsa

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

Command Modes Global configuration

Command History	Release	Modification
	11.3 T	This command was introduced.

Usage Guidelines Use this command to enter public key chain configuration mode. Use this command when you need to manually specify other IPsec peers' RSA public keys. You need to specify other peers' keys when you configure RSA encrypted nonces as the authentication method in an Internet Key Exchange policy at your peer router.

Examples The following example specifies the RSA public keys of two other IPsec peers. The remote peers use their IP address as their identity.

```
Router(config)# crypto key pubkey-chain rsa
Router(config-pubkey-chain)# addressed-key 10.5.5.1
Router(config-pubkey-key)# key-string
Router(config-pubkey)# 00302017 4A7D385B 1234EF29 335FC973
Router(config-pubkey)# 2DD50A37 C4F4B0FD 9DADE748 429618D5
Router(config-pubkey)# 18242BA3 2EDFBDD3 4296142A DDF7D3D8
Router(config-pubkey)# 08407685 2F2190A0 0B43F1BD 9A8A26DB
Router(config-pubkey)# 07953829 791FCDE9 A98420F0 6A82045B
Router(config-pubkey)# 90288A26 DBC64468 7789F76E EE21
Router(config-pubkey)# quit
Router(config-pubkey-key)# exit
Router(config-pubkey-chain)# addressed-key 10.1.1.2
Router(config-pubkey-key)# key-string
Router(config-pubkey)# 0738BC7A 2BC3E9F0 679B00FE 53987BCC
Router(config-pubkey)# 01030201 42DD06AF E228D24C 458AD228
Router(config-pubkey)# 58BB5DDD F4836401 2A2D7163 219F882E
Router(config-pubkey)# 64CE69D4 B583748A 241BED0F 6E7F2F16
Router(config-pubkey)# 0DE0986E DF02031F 4B0B0912 F68200C4
Router(config-pubkey)# C625C389 0BFF3321 A2598935 C1B1
Router(config-pubkey)# quit
Router(config-pubkey-key)# exit
Router(config-pubkey-chain)# exit
Router(config)#
```

Related Commands	Command	Description
	address	Specifies the IP address of the remote RSA public key of the remote peer you will manually configure.
	addressed-key	Specifies the RSA public key of the peer you will manually configure.
	key-string (IKE)	Specifies the RSA public key of a remote peer.
	named-key	Specifies which peer RSA public key you will manually configure.
	show crypto key pubkey-chain rsa	Displays peer RSA public keys stored on your router.

crypto key zeroize rsa

To delete all RSA keys from your router, use the **crypto key zeroize rsa** command in global configuration mode.

```
crypto key zeroize rsa [key-pair-label]
```

Syntax Description	<i>key-pair-label</i> (Optional) Specifies the name of the key pair that router will delete.
---------------------------	--

Defaults	No default behavior or values.
-----------------	--------------------------------

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	11.3 T	This command was introduced.
	12.2(8)T	The <i>key-pair-label</i> argument was added.

Usage Guidelines	<p>This command deletes all Rivest, Shamir, and Adelman (RSA) keys that were previously generated by your router unless you include the <i>key-pair-label</i> argument, which will delete only the specified RSA key pair. If you issue this command, you must also perform two additional tasks for each trustpoint that is associated with the key pair that was deleted:</p>
-------------------------	---

- Ask the certification authority (CA) administrator to revoke your router's certificates at the CA; you must supply the challenge password you created when you originally obtained the router's certificates using the **crypto ca enroll** command.
- Manually remove the router's certificates from the configuration by removing the configured trustpoint (using the **no crypto ca trustpoint name** command.)



Note

This command cannot be undone (after you save your configuration), and after RSA keys have been deleted, you cannot use certificates or the CA or participate in certificate exchanges with other IP Security (IPSec) peers unless you reconfigure CA interoperability by regenerating RSA keys, getting the CA's certificate, and requesting your own certificate again.

This command is not saved to the configuration.

Examples

The following example deletes the general-purpose RSA key pair that was previously generated for the router. After deleting the RSA key pair, the administrator contacts the CA administrator and requests that the certificate of the router be revoked. The administrator then deletes the certificate of the router from the configuration.

```
crypto key zeroize rsa
crypto ca certificate chain
no certificate
```

Related Commands

Command	Description
certificate	Adds certificates manually.
crypto ca certificate chain	Enters the certificate chain configuration mode.
crypto ca trustpoint	Declares the CA that your router should use.
show crypto ca timers	Specifies which key pair to associate with the certificate.

crypto keyring

To define a crypto keyring to be used during Internet Key Exchange (IKE) authentication, use the **crypto keyring** command in global configuration mode. To remove the keyring, use the **no** form of this command.

```
crypto keyring keyring-name [vrf fvr-f-name]
```

```
no crypto keyring keyring-name [vrf fvr-f-name]
```

Syntax Description

<i>keyring-name</i>	Name of the crypto keyring.
vrf <i>fvr-f-name</i>	(Optional) Front door virtual routing and forwarding (FVRF) name to which the keyring will be referenced. The <i>fvr-f-name</i> must match the FVRF name that was defined during virtual routing and forwarding (VRF) configuration.

Defaults

All the Internet Security Association and Key Management Protocol (ISAKMP) keys that were defined in the global configuration are part of the default global keyring.

Command Modes

Global configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

A keyring is a repository of preshared and Rivest, Shamir, and Adelman (RSA) public keys. The keyring is used in the isakmp profile configuration mode. The ISAKMP profile successfully completes authentication of peers if the peer keys are defined in the keyring that is attached to this profile.

Examples

The following example shows that a keyring and its usage have been defined:

```
crypto keyring vpnkeys
  pre-shared-key address 10.72.23.11 key vpnsecret
crypto isakmp profile vpnprofile
  keyring vpnkeys
```

crypto map (global IPsec)

To enter crypto map configuration mode and create or modify a crypto map entry, to create a crypto profile that provides a template for configuration of dynamically created crypto maps, or to configure a client accounting list, use the **crypto map** command in global configuration mode. To delete a crypto map entry, profile, or set, use the **no** form of this command.

crypto map *map-name seq-num* [**ipsec-manual**]

crypto map *map-name seq-num* [**ipsec-isakmp**] [**dynamic** *dynamic-map-name*] [**discover**]
[**profile** *profile-name*]

crypto map *map-name* [**client-accounting-list** *aaalist*]

no crypto map *map-name seq-num*



Note

Issue the **crypto map** *map-name seq-num* command without a keyword to modify an existing crypto map entry.

Syntax Description

<i>map-name</i>	Name that identifies the crypto map set. This is the name assigned when the crypto map was created.
<i>seq-num</i>	Sequence number you assign to the crypto map entry. See additional explanation for using this argument in the “Usage Guidelines” section.
ipsec-manual	(Optional) Indicates that Internet Key Exchange (IKE) will not be used to establish the IP Security (IPSec) security associations (SAs) for protecting the traffic specified by this crypto map entry.
ipsec-isakmp	(Optional) Indicates that IKE will be used to establish the IPSec SAs for protecting the traffic specified by this crypto map entry.
dynamic	(Optional) Specifies that this crypto map entry is to reference a preexisting dynamic crypto map. Dynamic crypto maps are policy templates used in processing negotiation requests from a peer IPSec device. If you use this keyword, none of the crypto map configuration commands will be available.
<i>dynamic-map-name</i>	(Optional) Specifies the name of the dynamic crypto map set that should be used as the policy template.
discover	(Optional) Enables peer discovery. By default, peer discovery is not enabled.
profile	(Optional) Designates a crypto map as a configuration template. The security configurations of this crypto map will be cloned as new crypto maps are created dynamically on demand.
<i>profile-name</i>	(Optional) Name of the crypto profile being created.
client-accounting-list	(Optional) Designates a client accounting list.
<i>aaalist</i>	(Optional) List name.

Defaults

No crypto maps exist.

Peer discovery is not enabled.

Command Modes Global configuration

Command History	Release	Modification
	11.2	This command was introduced.
	11.3 T	The following keywords and arguments were added: <ul style="list-style-type: none"> • ipsec-manual • ipsec-isakmp • dynamic • <i>dynamic-map-name</i>
	12.0(5)T	The discover keyword was added to support Tunnel Endpoint Discovery (TED).
	12.2(4)T	The profile <i>profile-name</i> keyword and argument combination was introduced to allow the generation of a crypto map profile that is cloned to create dynamically created crypto maps on demand.
	12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and support was added for the Cisco 1760, Cisco AS5300, Cisco AS5400, and Cisco AS5800 platforms.
	12.2(15)T	The client-accounting-list keyword and <i>aaalist</i> argument were added.

Usage Guidelines Use this command to create a new crypto map entry, to create a crypto map profile, or to modify an existing crypto map entry or profile.

After a crypto map entry has been created, you cannot change the parameters specified at the global configuration level because these parameters determine which of the configuration commands are valid at the crypto map level. For example, after a map entry has been created using the **ipsec-isakmp** keyword, you cannot change it to the option specified by the **ipsec-manual** keyword; you must delete and reenter the map entry.

After you define crypto map entries, you can assign the crypto map set to interfaces using the **crypto map** (interface IPSec) command.

Crypto Map Functions

Crypto maps provide two functions: filtering and classifying traffic to be protected and defining the policy to be applied to that traffic. The first use affects the flow of traffic on an interface; the second affects the negotiation performed (via IKE) on behalf of that traffic.

IPSec crypto maps define the following:

- What traffic should be protected
- To which IPSec peers the protected traffic can be forwarded—these are the peers with which an SA can be established
- Which transform sets are acceptable for use with the protected traffic
- How keys and security associations should be used or managed (or what the keys are, if IKE is not used)

Multiple Crypto Map Entries with the Same Map Name Form a Crypto Map Set

A crypto map set is a collection of crypto map entries, each with a different *seq-num* argument but the same *map-name* argument. Therefore, for a given interface, you could have certain traffic forwarded to one IPSec peer with specified security applied to that traffic and other traffic forwarded to the same or a different IPSec peer with different IPSec security applied. To accomplish differential forwarding you would create two crypto maps, each with the same *map-name* argument, but each with a different *seq-num* argument. Crypto profiles must have unique names within a crypto map set.

Sequence Numbers

The number you assign to the *seq-num* argument should not be arbitrary. This number is used to rank multiple crypto map entries within a crypto map set. Within a crypto map set, a crypto map entry with a lower *seq-num* is evaluated before a map entry with a higher *seq-num*; that is, the map entry with the lower number has a higher priority.

For example, consider a crypto map set that contains three crypto map entries: mymap 10, mymap 20, and mymap 30. The crypto map set named “mymap” is applied to serial interface 0. When traffic passes through serial interface 0, the traffic is evaluated first for mymap 10. If the traffic matches any access list permit statement entry in the extended access list in mymap 10, the traffic will be processed according to the information defined in mymap 10 (including establishing IPSec SAs when necessary). If the traffic does not match the mymap 10 access list, the traffic will be evaluated for mymap 20, and then mymap 30, until the traffic matches a permit entry in a map entry. (If the traffic does not match a permit entry in any crypto map entry, it will be forwarded without any IPSec security.)

Dynamic Crypto Maps

Refer to the “Usage Guidelines” section of the **crypto dynamic-map** command for a discussion on dynamic crypto maps.

Crypto map entries that reference dynamic map sets should be the lowest priority map entries, allowing inbound SA negotiation requests to try to match the static maps first. Only after the request does not match any of the static maps, do you want it to be evaluated against the dynamic map set.

To make a crypto map entry referencing a dynamic crypto map set the lowest priority map entry, give the map entry the highest *seq-num* of all the map entries in a crypto map set.

Create dynamic crypto map entries using the **crypto dynamic-map** command. After you create a dynamic crypto map set, add the dynamic crypto map set to a static crypto map set with the **crypto map** (global IPSec) command using the **dynamic** keyword.

TED

TED is an enhancement to the IPSec feature. Defining a dynamic crypto map allows you to dynamically determine an IPSec peer; however, only the receiving router has this ability. With TED, the initiating router can dynamically determine an IPSec peer for secure IPSec communications.

Dynamic TED helps to simplify IPSec configuration on the individual routers within a large network. Each node has a simple configuration that defines the local network that the router is protecting and the IPSec transforms that are required.



Note

TED helps only in discovering peers; otherwise, TED does not function any differently from normal IPSec. Thus, TED does not improve the scalability of IPSec (in terms of performance or the number of peers or tunnels).

Crypto Map Profiles

Crypto map profiles are created using the **profile** *profile-name* keyword and argument combination. Crypto map profiles are used as configuration templates for dynamically creating crypto maps on demand for use with the Layer 2 Transport Protocol (L2TP) Security feature. The relevant SAs the crypto map profile will be cloned and used to protect IP traffic on the L2TP tunnel.



Note

The **set peer** and **match address** commands are ignored by crypto profiles and should not be configured in the crypto map definition.

Examples

The following example shows the minimum required crypto map configuration when IKE will be used to establish the SAs:

```
crypto map mymap 10 ipsec-isakmp
  match address 101
  set transform-set my_t_set1
  set peer 10.0.0.1
```

The following example shows the minimum required crypto map configuration when the SAs are manually established:

```
crypto transform-set someset ah-md5-hmac esp-des
crypto map mymap 10 ipsec-manual
  match address 102
  set transform-set someset
  set peer 10.0.0.5
  set session-key inbound ah 256 98765432109876549876543210987654
  set session-key outbound ah 256 fedcbafedcbafedcfedcbafedcbafedc
  set session-key inbound esp 256 cipher 0123456789012345
  set session-key outbound esp 256 cipher abcdefabcdefabcd
```

The following example configures an IPSec crypto map set that includes a reference to a dynamic crypto map set.

Crypto map “mymap 10” allows SAs to be established between the router and either (or both) of two remote IPSec peers for traffic matching access list 101. Crypto map “mymap 20” allows either of two transform sets to be negotiated with the remote peer for traffic matching access list 102.

Crypto map entry “mymap 30” references the dynamic crypto map set “mydynamicmap,” which can be used to process inbound SA negotiation requests that do not match “mymap” entries 10 or 20. In this case, if the peer specifies a transform set that matches one of the transform sets specified in “mydynamicmap,” for a flow permitted by the access list 103, IPSec will accept the request and set up SAs with the remote peer without previously knowing about the remote peer. If the request is accepted, the resulting SAs (and temporary crypto map entry) are established according to the settings specified by the remote peer.

The access list associated with “mydynamicmap 10” is also used as a filter. Inbound packets that match any access list permit statement in this list are dropped for not being IPSec protected. (The same is true for access lists associated with static crypto maps entries.) Outbound packets that match a permit statement without an existing corresponding IPSec SA are also dropped.

```
crypto map mymap 10 ipsec-isakmp
  match address 101
  set transform-set my_t_set1
  set peer 10.0.0.1
  set peer 10.0.0.2
```

```

crypto map mymap 20 ipsec-isakmp
  match address 102
  set transform-set my_t_set1 my_t_set2
  set peer 10.0.0.3
crypto map mymap 30 ipsec-isakmp dynamic mydynamicmap
!
crypto dynamic-map mydynamicmap 10
  match address 103
  set transform-set my_t_set1 my_t_set2 my_t_set3

```

The following example configures TED on a Cisco router:

```
crypto map testtag 10 ipsec-isakmp dynamic dmap discover
```

The following example configures a crypto profile to be used as a template for dynamically created crypto maps when IPsec is used to protect an L2TP tunnel:

```
crypto map l2tpsec 10 ipsec-isakmp profile l2tp
```

Related Commands

Command	Description
crypto dynamic-map	Creates a dynamic crypto map entry and enters the crypto map configuration command mode.
crypto isakmp profile	Audits IPsec user sessions.
crypto map (interface IPsec)	Applies a previously defined crypto map set to an interface.
crypto map local-address	Specifies and names an identifying interface to be used by the crypto map for IPsec traffic.
debug crypto isakmp	Applies a previously defined crypto map set to an interface.
match address (IPsec)	Specifies an extended access list for a crypto map entry.
set peer (IPsec)	Specifies an IPsec peer in a crypto map entry.
set pfs	Specifies that IPsec should ask for PFS when requesting new SAs for this crypto map entry, or that IPsec requires PFS when receiving requests for new SAs.
set security-association level per-host	Specifies that separate IPsec SAs should be requested for each source/destination host pair.
set security-association lifetime	Overrides (for a particular crypto map entry) the global lifetime value, which is used when negotiating IPsec SAs.
set session-key	Specifies the IPsec session keys within a crypto map entry.
set transform-set	Specifies which transform sets can be used with the crypto map entry.
show crypto map (IPsec)	Displays the crypto map configuration.

crypto map (interface IPsec)

To apply a previously defined crypto map set to an interface, use the **crypto map** command in interface configuration mode. To remove the crypto map set from the interface, use the **no** form of this command.

```
crypto map map-name [redundancy standby-group-name [stateful]]
```

```
no crypto map [map-name] [redundancy standby-group-name [stateful]]
```

Syntax Description

<i>map-name</i>	Name that identifies the crypto map set. This is the name assigned when the crypto map was created. When the no form of the command is used, this argument is optional. Any value supplied for the argument is ignored.
redundancy	(Optional) Defines a backup IP Security (IPsec) peer. Both routers in the standby group are defined by the redundancy <i>standby name</i> and share the same virtual IP address.
<i>standby-group-name</i>	(Optional) Refers to the name of the standby group as defined by Hot Standby Router Protocol (HSRP) standby commands.
stateful	(Optional) Enables IPsec stateful failover for the crypto map.

Defaults

No crypto maps are assigned to interfaces.

Command Modes

Interface configuration

Command History

Release	Modification
11.2	This command was introduced.
12.1(9)E	The redundancy keyword and <i>standby-name</i> argument were added.
12.2(8)T	The redundancy keyword and <i>standby-name</i> argument were integrated into Cisco IOS Release 12.2(8)T.
12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5800 platforms.
12.2(9)YE	The redundancy keyword and <i>standby-name</i> argument were integrated into Cisco IOS Release 12.2(9)YE.
12.2(14)S	This feature was integrated into Cisco IOS Release 12.2(14)S.
12.3(11)T	The stateful keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Use this command to assign a crypto map set to an interface. You must assign a crypto map set to an interface before that interface can provide IPsec services. Only one crypto map set can be assigned to an interface. If multiple crypto map entries have the same map name but a different sequence number, they are considered to be part of the same set and will all be applied to the interface. The crypto map

entry that has the lowest sequence number is considered the highest priority and will be evaluated first. A single crypto map set can contain a combination of **ipsec-isakmp** and **ipsec-manual crypto map** entries.



Note A crypto map applied to loopback interface is not supported.

The standby name must be configured on all devices in the standby group, and the standby address must be configured on at least one member of the group. If the standby name is removed from the router, the IPSec security associations (SAs) will be deleted. If the standby name is added again, regardless of whether the same name or a different name is used, the crypto map (using the **redundancy** option) will have to be reapplied to the interface.



Note A virtual IP address must be configured in the standby group to enable either stateless or stateful redundancy.

The **stateful** keyword enables stateful failover of IKE and IPSec sessions. Stateful Switchover (SSO) must also be configured for IPSec stateful failover to operate correctly.

Examples

The following example shows how all remote Virtual Private Network (VPN) gateways connect to the router via 192.168.0.3:

```
crypto map mymap 1 ipsec-isakmp
  set peer 10.1.1.1
  reverse-route
  set transform-set esp-3des-sha
  match address 102
```

```
Interface FastEthernet 0/0
ip address 192.168.0.2 255.255.255.0
standby name group1
standby ip 192.168.0.3
crypto map mymap redundancy group1
```

```
access-list 102 permit ip 192.168.1.0 0.0.0.255 10.0.0.0 0.0.255.255
```

The crypto map on the interface binds this standby address as the local tunnel endpoint for all instances of “mymap” and, at the same time, ensures that stateless HSRP failover is facilitated between an active and standby device that belongs to the same standby group, “group1.”

Reverse route injection (RRI) is also enabled to provide the ability for only the *active* device in the HSRP group to be advertising itself to inside devices as the next hop VPN gateway to the remote proxies. If a failover occurs, routes are deleted on the former active device and created on the new active device.

The following example shows how to configure IPSec stateful failover on the crypto map “to-peer-outside”:

```
crypto map to-peer-outside 10 ipsec-isakmp
  set peer 209.165.200.225
  set transform-set trans1
  match address peer-outside
```

```
interface Ethernet0/0
ip address 209.165.201.1 255.255.255.224
standby 1 ip 209.165.201.3
standby 1 preempt
standby 1 name HA-out
```

```
standby 1 track Ethernet1/0
crypto map to-peer-outside redundancy HA-out stateful
```

Related Commands

Command	Description
crypto map (global IPSec)	Creates or modifies a crypto map entry and enters the crypto map configuration mode.
crypto map local-address	Specifies and names an identifying interface to be used by the crypto map for IPSec traffic.
redundancy inter-device	Configures redundancy and enters inter-device configuration mode.
show crypto map (IPSec)	Displays the crypto map configuration.
standby ip	Assigns an IP address that is to be shared among the members of the HSRP group and owned by the primary IP address.
standby name	Assigns a user-defined group name to the HSRP redundancy group.

crypto map client authentication list

To configure Internet Key Exchange extended authentication (Xauth) on your router, use the **crypto map client authentication list** command in global configuration mode. To restore the default value, use the **no** form of this command.

crypto map *map-name* **client authentication list** *list-name*

no crypto map *map-name* **client authentication list** *list-name*

Syntax Description		
	<i>map-name</i>	The name you assign to the crypto map set.
	<i>list-name</i>	Character string used to name the list of authentication methods activated when a user logs in. The list-name must match the list-name defined during AAA configuration.

Defaults Xauth is not enabled.

Command Modes Global configuration

Command History	Release	Modification
	12.1(1)T	This command was introduced.

Usage Guidelines Before configuring Xauth, you should complete the following tasks:

- Set up an authentication list using AAA commands.
- Configure an IP Security transform.
- Configure a crypto map.
- Configure Internet Security Association Key Management Protocol (ISAKMP) policy.

After enabling Xauth, you should apply the crypto map on which Xauth is configured to the router interface.

Examples The following example configures user authentication (a list of authentication methods called *xauthlist*) on an existing static crypto map called *xauthmap*:

```
crypto map xauthmap client authentication list xauthlist
```

The following example configures user authentication (a list of authentication methods called *xauthlist*) on a dynamic crypto map called *xauthdynamic* that has been applied to a static crypto map called *xauthmap*:

```
crypto map xauthmap client authentication list xauthlist
crypto map xauthmap 10 ipsec-isakmp dynamic xauthdynamic
```

Related Commands	Command	Description
	aaa authentication login	Sets AAA authentication at login.
	crypto ipsec transform-set	Defines a transform set, which is an acceptable combination of security protocols and algorithms, and enters crypto transform configuration mode.
	crypto isakmp key	Configures a preshared authentication key.
	crypto isakmp policy	Defines an IKE policy, and enters ISAKMP policy configuration mode.
	crypto map (global configuration)	Creates or modify a crypto map entry, and enters the crypto map configuration mode.
	interface	Enters the interface configuration mode.

crypto map client configuration address

To configure IKE Mode Configuration on your router, use the **crypto map client configuration address** command in global configuration mode. To disable IKE Mode Configuration, use the **no** form of this command.

crypto map tag client configuration address [initiate | respond]

no crypto map tag client configuration address

Syntax Description		
	<i>tag</i>	The name that identifies the crypto map.
	initiate	(Optional) A keyword that indicates the router will attempt to set IP addresses for each peer.
	respond	(Optional) A keyword that indicates the router will accept requests for IP addresses from any requesting peer.

Defaults IKE Mode Configuration is not enabled.

Command Modes Global configuration

Command History	Release	Modification
	12.0(4)XE	This command was introduced.
	12.0(7)T	This command was implemented in Cisco IOS release 12.0(7)T.

Usage Guidelines At the time of this publication, this feature is an IETF draft with limited support. Therefore this feature was not designed to enable the configuration mode for every IKE connection by default.

Examples The following examples configure IKE Mode Configuration on your router:

```
crypto map dyn client configuration address initiate
crypto map dyn client configuration address respond
```

Related Commands	Command	Description
	crypto map (global)	Creates or modifies a crypto map entry and enters the crypto map configuration mode

crypto map isakmp authorization list

To enable Internet Key Exchange (IKE) querying of authentication, authorization, and accounting (AAA) for tunnel attributes in aggressive mode, use the **crypto map isakmp authorization list** command in global configuration mode. To restore the default value, use the **no** form of this command.

crypto map *map-name* **isakmp authorization list** *list-name*

no crypto map *map-name* **isakmp authorization list** *list-name*

Syntax Description		
	<i>map-name</i>	Name you assign to the crypto map set.
	<i>list-name</i>	Character string used to name the list of authorization methods activated when a user logs in. The list name must match the list name defined during AAA configuration.

Defaults No default behavior or values.

Command Modes Global configuration

Command History	Release	Modification
	12.1(1)T	This command was introduced

Usage Guidelines Use the **crypto map client authorization list** command to enable key lookup from a AAA server.

Preshared keys deployed in a large-scale Virtual Private Network (VPN) without a certification authority, with dynamic IP addresses, are accessed during aggression mode of IKE negotiation through a AAA server. Thus, users have their own key, which is stored on an external AAA server. This allows for central management of the user database, linking it to an existing database, in addition to allowing every user to have their own unique, more secure pre-shared key.

Before configuring the **crypto map client authorization list** command, you should perform the following tasks:

- Set up an authorization list using AAA commands.
- Configure an IPSec transform.
- Configure a crypto map.
- Configure an Internet Security Association Key Management Protocol policy using IPSec and IKE commands.

After enabling the **crypto map client authorization list** command, you should apply the previously defined crypto map to the interface.

Examples

The following example shows how to configure the **crypto map client authorization list** command:

```
crypto map ikessaaamap isakmp authorization list ikessaaalist
crypto map ikessaaamap 10 ipsec-isakmp dynamic ikessaaadyn
```

Related Commands

Command	Description
aaa authorization	Sets parameters that restrict a user's network access.
crypto ipsec transform-set	Defines a transform set, which is an acceptable combination of security protocols and algorithms, and enters crypto transform configuration mode.
crypto map (global configuration)	Creates or modifies a crypto map entry and enters the crypto map configuration mode
crypto isakmp policy	Defines an IKE policy and enters ISAKMP policy configuration mode.
crypto isakmp key	Configures a preshared authentication key.
interface	Enters interface configuration mode.

crypto map isakmp-profile

To configure an Internet Security Association and Key Management Protocol (ISAKMP) profile on a crypto map, use the **crypto map isakmp-profile** command in global configuration mode. To restore the default values on the crypto map, use the **no** form of this command.

```
crypto map map-name isakmp-profile isakmp-profile-name
```

```
no crypto map map-name isakmp-profile isakmp-profile-name
```

Syntax Description

<i>map-name</i>	Name assigned to the crypto map set.
<i>isakmp-profile-name</i>	Character string used to name the ISAKMP profile that is used during an Internet Key Exchange (IKE) Phase 1 and Phase 1.5 exchange. The <i>isakmp-profile-name</i> must match the ISAKMP profile name that was defined during the ISAKMP profile configuration.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

This command describes the ISAKMP profile to use to start the IKE exchange. Before configuring this command, you must set up the ISAKMP profile.

Examples

The following example shows that an ISAKMP profile is configured on a crypto map:

```
crypto map vpnmap isakmp-profile vpnprofile
```

Related Commands

Command	Description
crypto ipsec transform-set	Defines a transform set—an acceptable combination of security protocols and algorithms.
crypto map (global)	Creates or modifies a crypto map entry.

crypto map local-address

To specify and name an identifying interface to be used by the crypto map for IPsec traffic, use the **crypto map local-address** command in global configuration mode. To remove this command from the configuration, use the **no** form of this command.

crypto map *map-name* **local-address** *interface-id*

no crypto map *map-name* **local-address**

Syntax Description

<i>map-name</i>	Name that identifies the crypto map set. This is the name assigned when the crypto map was created.
<i>interface-id</i>	The identifying interface that should be used by the router to identify itself to remote peers. If Internet Key Exchange is enabled and you are using a certification authority (CA) to obtain certificates, this should be the interface with the address specified in the CA certificates.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
11.3 T	This command was introduced.

Usage Guidelines

If you apply the same crypto map to two interfaces and do not use this command, two separate security associations (with different local IP addresses) could be established to the same peer for similar traffic. If you are using the second interface as redundant to the first interface, it could be preferable to have a single security association (with a single local IP address) created for traffic sharing the two interfaces. Having a single security association decreases overhead and makes administration simpler.

This command allows a peer to establish a single security association (and use a single local IP address) that is shared by the two redundant interfaces.

If applying the same crypto map set to more than one interface, the default behavior is as follows:

- Each interface will have its own security association database.
- The IP address of the local interface will be used as the local address for IPsec traffic originating from/destined to that interface.

However, if you use a local-address for that crypto map set, it has multiple effects:

- Only one IPsec security association database will be established and shared for traffic through both interfaces.
- The IP address of the specified interface will be used as the local address for IPsec (and IKE) traffic originating from or destined to that interface.

One suggestion is to use a loopback interface as the referenced local address interface, because the loopback interface never goes down.

Examples

The following example assigns crypto map set “mymap” to the S0 interface and to the S1 interface. When traffic passes through either S0 or S1, the traffic will be evaluated against the all the crypto maps in the “mymap” set. When traffic through either interface matches an access list in one of the “mymap” crypto maps, a security association will be established. This same security association will then apply to both S0 and S1 traffic that matches the originally matched IPSec access list. The local address that IPSec will use on both interfaces will be the IP address of interface loopback0.

```
interface S0
  crypto map mymap

interface S1
  crypto map mymap

crypto map mymap local-address loopback0
```

Related Commands

Command	Description
crypto map (interface IPSec)	Applies a previously defined crypto map set to an interface.

crypto mib ipsec flowmib history failure size

To change the size of the IP Security (IPSec) MIB failure history table, use the **crypto mib ipsec flowmib history failure size** command in global configuration mode.

crypto mib ipsec flowmib history failure size *number*

Syntax Description	<i>number</i>	Size of the failure history table. The default value is 200.
---------------------------	---------------	--

Defaults The default table size is 200.

Command Modes Global configuration

Command History	Release	Modification
	12.1(4)E	This command was introduced.
	12.2(4)T	This command was integrated into Cisco IOS Release 12.2 T.

Usage Guidelines Use the **crypto mib ipsec flowmib history failure size** command to change the size of a failure history table. If you do not configure the size of a failure history table, the default of 200 will be implemented. A failure history table stores the reason for tunnel failure and the time failure occurred. A failure history table can be used as a simple method to distinguish between a normal and an abnormal tunnel termination. That is, if a tunnel entry in the tunnel history table has no associated failure record, the tunnel must have terminated normally. However, every failure does not correspond to a tunnel. Supported setup failures are recorded in the failure table, but a history table is not associated because a tunnel was never set up.

Examples In the following example, the size of a failure history table is configured to be 140:

```
Router(config)# crypto mib ipsec flowmib history failure size 140
```

Related Commands	Command	Description
	crypto mib ipsec flowmib history tunnel size	Changes the size of the IPSec tunnel history table.
	show crypto mib ipsec flowmib history failure size	Displays the size of the IPSec failure history table.

crypto mib ipsec flowmib history tunnel size

To change the size of the IP Security (IPSec) tunnel history table, use the **crypto mib ipsec flowmib history tunnel size** command in global configuration mode.

crypto mib ipsec flowmib history tunnel size *number*

Syntax Description	<i>number</i>	Size of the tunnel history table. The default value is 200.
---------------------------	---------------	---

Defaults The default table size is 200.

Command Modes Global configuration

Command History	Release	Modification
	12.1(4)E	This command was introduced.
	12.2(4)T	This command was integrated into Cisco IOS Release 12.2 T.

Usage Guidelines Use the **crypto mib ipsec flowmib history tunnel size** command to change the size of a tunnel history table. If you do not configure the size of a tunnel history table, the default of 200 will be implemented. A tunnel history table stores the attribute and statistics records, which contain the attributes and the last snapshot of the traffic statistics of a given tunnel. A tunnel history table accompanies a failure table, so you can display the complete history of a given tunnel. However, a tunnel history table does not accompany every failure table because every failure does not correspond to a tunnel. Thus, supported setup failures are recorded in the failure table, but an associated history table is not recorded because a tunnel was never set up.

As an optimization, a tunnel endpoint table can be combined with a tunnel history table. However, if a tunnel endpoint table is combined, all three tables (the failure history table, tunnel history table, and the endpoint table) must remain the same size even though the MIB allows each table to be distinct.

Examples In the following example, the size of the tunnel history table changed to 130:

```
Router(config)# crypto mib ipsec flowmib history tunnel size 130
```

crypto pki crl request

To request that a new certificate revocation list (CRL) be obtained immediately from the certification authority, use the **crypto pki crl request** command in global configuration mode.

crypto pki crl request *name*

Syntax Description	<i>name</i>	Specifies the name of the CA. This is the same name used when the CA was declared with the crypto pki trustpoint command.
---------------------------	-------------	--

Defaults Normally, the router requests a new CRL when it is verifying a certificate and there is no CRL cached.

Command Modes Global configuration

Command History	Release	Modification
	11.3 T	The crypto ca crl request command was introduced.
	12.3(7)T	This command replaced the crypto ca crl request command.

Usage Guidelines A CRL lists all the certificates of the network device that have been revoked. Revoked certificates will not be honored by your router; therefore, any IPSec device with a revoked certificate cannot exchange IP Security traffic with your router.

The first time your router receives a certificate from a peer, it will download a CRL from the CA. Your router then checks the CRL to make sure the certificate of the peer has not been revoked. (If the certificate appears on the CRL, it will not accept the certificate and will not authenticate the peer.)

A CRL can be reused with subsequent certificates until the CRL expires. If your router receives the certificate of a peer after the applicable CRL has expired, it will download the new CRL.

If your router has a CRL which has not yet expired, but you suspect that the contents of the CRL are out of date, use the **crypto pki crl request** command to request that the latest CRL be immediately downloaded to replace the old CRL.

This command is not saved to the configuration.



Note

This command should be used only after the trustpoint is enrolled.

Examples The following example immediately downloads the latest CRL to your router:

```
crypto pki crl request
```

crypto pki trustpoint

To declare the certification authority (CA) that your router should use, use the **crypto pki trustpoint** command in global configuration mode. To delete all identity information and certificates associated with the CA, use the **no** form of this command.

crypto pki trustpoint *name*

no crypto pki trustpoint *name*

Syntax Description

<i>name</i>	Creates a name for the CA. (If you previously declared the CA and just want to update its characteristics, specify the name you previously created.)
-------------	--

Defaults

Your router does not recognize any CAs until you declare a CA using this command.

Command Modes

Global configuration

Command History

Release	Modification
12.3(7)T	This command replaced the crypto ca trustpoint command. You can still enter the crypto ca trustpoint command, but the command will be written in the configuration as “crypto pki trustpoint.”

Usage Guidelines

Use the **crypto pki trustpoint** command to declare a CA, which can be a self-signed root CA or a subordinate CA. Issuing the **crypto pki trustpoint** command puts you in ca-trustpoint configuration mode.

You can specify characteristics for the trustpoint CA using the following subcommands:

- **crl**—Queries the certificate revocation list (CRL) to ensure that the certificate of the peer has not been revoked.
- **default (ca-trustpoint)**—Resets the value of ca-trustpoint configuration mode subcommands to their defaults.
- **enrollment**—Specifies enrollment parameters (optional).
- **enrollment http-proxy**—Accesses the CA by HTTP through the proxy server.
- **match certificate**—Associates a certificate-based access control list (ACL) defined with the **crypto ca certificate map** command.
- **primary**—Assigns a specified trustpoint as the primary trustpoint of the router.
- **root**—Defines the Trivial File Transfer Protocol (TFTP) to get the CA certificate and specifies both a name for the server and a name for the file that will store the CA certificate.

The following example shows how to declare the CA named “ka” and specify enrollment and CRL parameters:

```
crypto pki trustpoint ka
enrollment url http://kahului:80
```

The following example shows a certificate-based access control list (ACL) with the label “Group” defined in a **crypto ca certificate map** command and included in the **match certificate** subcommand of the **crypto pki trustpoint** command:

```
crypto ca certificate map Group 10
  subject-name co ou=WAN
  subject-name co o=Cisco
!
crypto pki trustpoint pkil
  match certificate Group
```

Related Commands

Command	Description
crl	Queries the CRL to ensure that the certificate of the peer has not been revoked.
default (ca-trustpoint)	Resets the value of a ca-trustpoint configuration subcommand to its default.
enrollment	Specifies the enrollment parameters of your CA.
enrollment http-proxy	Accesses the CA by HTTP through the proxy server.
primary	Assigns a specified trustpoint as the primary trustpoint of the router.
root	Obtains the CA certificate via TFTP.

ctype

To preauthenticate calls on the basis of the call type, use the **ctype** command in AAA preauthentication configuration mode. To remove the **ctype** command from your configuration, use the **no** form of this command.

ctype [**if-avail** | **required**] [**accept-stop**] [**password** *password*] [**digital** | **speech** | **v.110** | **v.120**]

no ctype [**if-avail** | **required**] [**accept-stop**] [**password** *password*] [**digital** | **speech** | **v.110** | **v.120**]

Syntax Description

if-avail	(Optional) Implies that if the switch provides the data, RADIUS must be reachable and must accept the string in order for preauthentication to pass. If the switch does not provide the data, preauthentication passes.
required	(Optional) Implies that the switch must provide the associated data, that RADIUS must be reachable, and that RADIUS must accept the string in order for preauthentication to pass. If these three conditions are not met, preauthentication fails.
accept-stop	(Optional) Prevents subsequent preauthentication elements such as clid or dnis from being tried once preauthentication has succeeded for a call element.
password <i>password</i>	(Optional) Defines the password for the preauthentication element.
digital	(Optional) Specifies “digital” as the call type for preauthentication.
speech	(Optional) Specifies “speech” as the call type for preauthentication.
v.110	(Optional) Specifies “v.110” as the call type for preauthentication.
v.120	(Optional) Specifies “v.120” as the call type for preauthentication.

Defaults

The **if-avail** and **required** keywords are mutually exclusive. If the **if-avail** keyword is not configured, the preauthentication setting defaults to **required**.

The default password string is cisco.

Command Modes

AAA preauthentication configuration

Command History

Release	Modification
12.1(2)T	This command was introduced.

Usage Guidelines

You may configure more than one of the AAA preauthentication commands (**clid**, **ctype**, **dnis**) to set conditions for preauthentication. The sequence of the command configuration decides the sequence of the preauthentication conditions. For example, if you configure **dnis**, then **clid**, then **ctype**, in this order, then this is the order of the conditions considered in the preauthentication process.

In addition to using the preauthentication commands to configure preauthentication on the Cisco router, you must set up the preauthentication profiles on the RADIUS server.

Set up the RADIUS preauthentication profile with the call type string as the username and with the password that is defined in the **ctype** command as the password. [Table 13](#) shows the call types that you may use in the preauthentication profile.

Table 13 Preauthentication Call Types

Call Type String	ISDN Bearer Capabilities
digital	Unrestricted digital, restricted digital.
speech	Speech, 3.1 kHz audio, 7 kHz audio.
v.110	Anything with V.110 user information layer.
v.120	Anything with V.120 user information layer.

Examples

The following example specifies that incoming calls be preauthenticated on the basis of the call type:

```
aaa preauth
 group radius
 ctype required
```

Related Commands

Command	Description
clid	Preauthenticates calls on the basis of the CLID number.
dnis (RADIUS)	Preauthenticates calls on the basis of the DNIS number.
dnis bypass (AAA preauthentication configuration)	Specifies a group of DNIS numbers that will be bypassed for preauthentication.
group (RADIUS)	Specifies the AAA RADIUS server group to use for preauthentication.