

reverse-route

To create source proxy information for a crypto map entry, use the **reverse-route** command in crypto map configuration mode. To remove the source proxy information from a crypto map entry, use the **no** form of this command.

reverse-route [**remote-peer** [*ip-address*]]

no reverse-route [**remote-peer** [*ip-address*]]

Syntax Description

remote-peer	(Optional) Routes of public IP addresses and IP security (IPSec) tunnel destination addresses are inserted into the routing table.
<i>ip-address</i>	(Optional) IP address of the next hop destination.

Defaults

No default behavior or values.

Command Modes

Crypto map configuration

Command History

Release	Modification
12.1(9)E	This command was introduced.
12.2(8)T	This command was 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(13)T	The remote-peer keyword was added.
12.3	The <i>ip-address</i> argument was added.

Usage Guidelines

This command can be applied on a per-crypto basis.

Reverse route injection (RRI) provides a scaleable mechanism to dynamically learn and advertise the IP address and subnets that belong to a remote site that connects through an IP Security (IPSec) virtual private network (VPN) tunnel.

When enabled in an IPSec crypto map, RRI will learn all the subnets from any network that is defined in the crypto access control list (ACL) as the destination network. The learned routes are installed into the local routing table as static routes that point to the encrypted interface. When the IPSec tunnel is torn down, the associated static routes will be removed. These static routes may then be redistributed into other dynamic routing protocols so that they can be advertised to other parts of the network (usually done by redistributing RRI routes into dynamic routing protocols on the core side).

Examples

The following example shows how all remote 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

```

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.
show crypto map (IPSec)	Displays the crypto map configuration.

root

To obtain the certification authority (CA) certificate via TFTP, use the **root** command in ca-trustpoint configuration mode. To deconfigure the CA, use the **no** form of this command.

```
root tftp server-hostname filename
```

```
no root tftp server-hostname filename
```

Syntax Description

tftp	Defines the TFTP protocol to get the root certificate.
<i>server-hostname</i>	Specifies a name for the server and a name for the file that will store the trustpoint CA.
<i>filename</i>	

Defaults

A CA certificate is not configured.

Command Modes

Ca-trustpoint configuration

Command History

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

Usage Guidelines

This command allows you to access the CA via the TFTP protocol, which is used to get the CA. You want to configure a CA certificate so that your router can verify certificates issued to peers. Thus, your router does not have to enroll with the CA that issued the certificates the peers.

Before you can configure this command, you must enable the **crypto ca trustpoint** command, which puts you in ca-trustpoint configuration mode.



Note

The **crypto ca trustpoint** command deprecates the **crypto ca identity** and **crypto ca trusted-root** commands and all related subcommands (all ca-identity and trusted-root configuration mode commands). If you enter a ca-identity or trusted-root subcommand, the configuration mode and command will be written back as ca-trustpoint.

Examples

The following example shows how to configure the CA certificate named “bar” using TFTP:

```
crypto ca trustpoint bar
root tftp xxx fff
crl optional
```

Related Commands

Command	Description
crypto ca trustpoint	Declares the CA that your router should use.

root CEP

The **crypto ca trustpoint** command deprecates the **crypto ca trusted-root** command and all related subcommands (all trusted-root configuration mode commands). If you enter a trusted-root subcommand, the configuration mode and command will be written back as ca-trustpoint.

root PROXY

The **root PROXY** command is replaced by the **enrollment http-proxy** command. See the **enrollment http-proxy** command for more information.

root TFTP

The **root TFTP** command is replaced by the **root** command. See the **root** command for more information.

rsakeypair

To specify which key pair to associate with the certificate, use the **rsakeypair** command in ca-trustpoint configuration mode.

```
rsakeypair key-label [key-size [encryption-key-size]]
```

Syntax Description

<i>key-label</i>	Name of the key pair, which is generated during enrollment if it does not already exist or if the auto-enroll regenerate command is configured.
<i>key-size</i>	(Optional) Size of the desired Rivest, Shamir, Adelman (RSA) key. If not specified, the existing key size is used.
<i>encryption-key-size</i>	(Optional) Size of the second key, which is used to request separate encryption, signature keys, and certificates.

Defaults

The fully qualified domain name (FQDN) key is used.

Command Modes

Ca-trustpoint configuration

Command History

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

Usage Guidelines

When you regenerate a key pair, you are responsible for reenrolling the identities associated with the key pair. Use the **rsakeypair** command to refer back to the named key pair.

Examples

The following example is a sample trustpoint configuration that specifies the RSA key pair “exampleCAkeys”:

```
crypto ca trustpoint exampleCAkeys
enroll url http://exampleCAkeys/certsrv/mscep/mscep.dll
rsakeypair exampleCAkeys 1024 1024
```

Related Commands

Command	Description
auto-enroll	Enables autoenrollment.
crl	Generates RSA key pairs.
crypto ca trustpoint	Declares the CA that your router should use.

rsa-pubkey

To define the Rivest, Shamir, and Adelman (RSA) manual key to be used for encryption or signature during Internet Key Exchange (IKE) authentication, use the **rsa-pubkey** command in keyring configuration mode. To remove the manual key that was defined, use the **no** form of this command.

```
rsa-pubkey {address address | name fqdn} [encryption | signature]
```

```
no rsa-pubkey {address address | name fqdn} [encryption | signature]
```

Syntax Description

address <i>address</i>	IP address of the remote peer.
name <i>fqdn</i>	Fully qualified domain name (FQDN) of the peer.
encryption	(Optional) The manual key is to be used for encryption.
signature	(Optional) The manual key is to be used for signature.

Defaults

No default behavior or values

Command Modes

Keyring configuration

Command History

Release	Modification
12.2(15)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 RSA public keys of other IP Security (IPSec) peers. You need to specify the keys of other peers when you configure RSA encrypted nonces as the authentication method in an IKE policy at your peer router.

Examples

The following example shows that the RSA public key of an IPSec peer has been specified:

```
Router(config)# crypto keyring vpnkeyring
Router(conf-keyring)# rsa-pubkey name host.vpn.com
Router(config-pubkey-key)# address 10.5.5.1
Router(config-pubkey)# 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(conf-keyring)# exit
```

security authentication failure rate

To configure the number of allowable unsuccessful login attempts, use the **security authentication failure rate** command in global configuration mode. To disable this functionality, use the **no** form of this command.

security authentication failure rate *threshold-rate* **log**

no security authentication failure rate *threshold-rate* **log**

Syntax Description

<i>threshold-rate</i>	Number of allowable unsuccessful login attempts. The valid value range for the <i>threshold-rate</i> argument is 2 to 1024. The default is 10.
log	Syslog authentication failures if the rate exceeds the threshold.

Defaults

The default number of failed login attempts before a 15-second delay is 10.

Command Modes

Global configuration

Command History

Release	Modification
12.3(1)	This command was introduced.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.3(7)T	The range of the <i>threshold-rate</i> value was changed from 1 through 1024 to 2 through 1024.

Usage Guidelines

The **security authentication failure rate** command provides enhanced security access to the router by generating syslog messages after the number of unsuccessful login attempts exceeds the configured threshold rate. This command ensures that there are not any continuous failures to access the router.



Note

Previous to the Cisco IOS software release 12.3(7)T the *threshold-rate* value range was 1 through 1024. Unsuccessful login attempts will not be logged if a value of 1 is configured. As of Cisco IOS release 12.3(7)T, use a value between 2 and 1024.

Examples

The following example shows how to configure your router to generate a syslog message after eight failed login attempts:

```
security authentication failure rate 8 log
```

Related Commands

Command	Description
security passwords min-length	Ensures that all configured passwords are at least a specified length.

security passwords min-length

To ensure that all configured passwords are at least a specified length, use the **security passwords min-length** command in global configuration mode. To disable this functionality, use the **no** form of this command.

security passwords min-length *length*

no security passwords min-length *length*

Syntax Description

length Minimum length of a configured password. The default is six characters.

Defaults

Six characters

Command Modes

Global configuration

Command History

Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines

The **security passwords min-length** command provides enhanced security access to the router by allowing you to specify a minimum password length, eliminating common passwords that are prevalent on most networks, such as “lab” and “cisco.” This command affects user passwords, enable passwords and secrets, and line passwords. After this command is enabled, any password that is less than the specified length will fail.

Examples

The following example shows both how to specify a minimum password length of six characters and what happens when the password does not adhere to the minimum length:

```
security password min-length 6
enable password lab
% Password too short - must be at least 6 characters. Password not configured.
```

Related Commands

Command	Description
enable password	Sets a local password to control access to various privilege levels.
security authentication failure rate	Configures the number of allowable unsuccessful login attempts.

self-identity

To define the identity that the local Internet Key Exchange (IKE) uses to identify itself to the remote peer, use the **self-identity** command in ISAKMP profile configuration mode. To remove the Internet Security Association and Key Management Protocol (ISAKMP) identity that was defined for the IKE, use the **no** form of this command.

```
self-identity { address | fqdn | user-fqdn user-fqdn }
```

```
no self-identity { address | fqdn | user-fqdn user-fqdn }
```

Syntax Description

address	The IP address of the local endpoint.
fqdn	The fully qualified domain name (FQDN) of the host.
user-fqdn <i>user-fqdn</i>	The user FQDN that is sent to the remote endpoint.

Defaults

If no ISAKMP identity is defined in the ISAKMP profile configuration, global configuration is the default.

Command Modes

ISAKMP profile configuration

Command History

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

Examples

The following example shows that the IKE identity is the user FQDN “user@vpn.com”:

```
crypto isakmp profile vpnprofile
 self-identity user-fqdn user@vpn.com
```

serial-number (ca-trustpoint)

To specify whether the router serial number should be included in the certificate request, use the **serial-number** command in ca-trustpoint configuration mode. To restore the default behavior, use the **no** form of this command.

serial-number [**none**]

no serial-number

Syntax Description

none	(Optional) Specifies that a serial number will not be included in the certificate request.
-------------	--

Defaults

Not configured. You will be prompted for the serial number during certificate enrollment.

Command Modes

Ca-trustpoint configuration

Command History

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

Usage Guidelines

Before you can issue the **serial-number** command, you must enable the **crypto ca trustpoint** command, which declares the certification authority (CA) that your router should use and enters ca-trustpoint configuration mode.

Use this command to specify the router serial number in the certificate request, or use the **none** keyword to specify that a serial number should not be included in the certificate request.

Examples

The following example shows how to include the router serial number in the "root" certificate request:

```
crypto ca trustpoint root
  enrollment url http://10.3.0.7:80
  ip-address none
  fqdn none
  serial-number none
  subject-name CN=jack, OU=PKI, O=Cisco Systems, C=US
```

The router will not prompt for the serial number during enrollment:

```
crypto ca trustpoint root
  enrollment url http://10.3.0.7:80
  serial-number
```

Related Commands

Command	Description
crypto ca trustpoint	Declares the CA that your router should use.

serial-number (pubkey)

To define the serial number for the Rivest, Shamir, and Adelman (RSA) manual key to be used for encryption or signatures during Internet Key Exchange (IKE) authentication, use the **serial-number** command in pubkey configuration mode. To remove the manual key that was defined, use the **no** form of this command.

serial-number *serial-number*

no serial-number *serial-number*

Syntax Description	<i>serial-number</i>	Device serial number. The value is from 0 through infinity.
---------------------------	----------------------	---

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

Command Modes	Pubkey configuration
----------------------	----------------------

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

Examples The following example shows that the public key of an IP Security (IPSec) peer has been specified:

```
Router(config)# crypto keyring vpnkeyring
Router(conf-keyring)# rsa-pubkey name host.vpn.com
Router(config-pubkey-key)# address 10.5.5.1
Router(config-pubkey-key)# serial-number 1000000
Router(config-pubkey)# 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(conf-keyring)# exit
```

Related Commands	Command	Description
	address	Specifies the IP address of the remote RSA public key of the remote peer that you will manually configure.
	key-string (IKE)	Specifies the RSA public key of a remote peer.

server (RADIUS)

To configure the IP address of the RADIUS server for the group server, use the **server** command in server-group configuration mode. To remove the associated server from the authentication, authorization, and accounting (AAA) group server, use the **no** form of this command.

```
server ip-address [auth-port port-number] [acct-port port-number]
```

```
no server ip-address [auth-port port-number] [acct-port port-number]
```

Syntax Description

<i>ip-address</i>	IP address of the RADIUS server host.
auth-port <i>port-number</i>	(Optional) Specifies the User Datagram Protocol (UDP) destination port for authentication requests. The port-number argument specifies the port number for authentication requests. The host is not used for authentication if this value is set to 0.
acct-port <i>port-number</i>	(Optional) Specifies the UDP destination port for accounting requests. The port number argument specifies the port number for accounting requests. The host is not used for accounting services if this value is set to 0.

Defaults

If no port attributes are defined, the defaults are as follows:

- Authentication port: 1645
- Accounting port: 1646

Command Modes

Server-group configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.0(7)T	The following new keywords/arguments were added: <ul style="list-style-type: none"> • auth-port <i>port-number</i> • acct-port <i>port-number</i>

Usage Guidelines

Use the **server** command to associate a particular server with a defined group server. There are two different ways in which you can identify a server, depending on the way you want to offer AAA services. You can identify the server simply by using its IP address, or you can identify multiple host instances or entries using the optional **auth-port** and **acct-port** keywords.

When you use the optional keywords, the network access server identifies RADIUS security servers and host instances associated with a group server on the basis of their IP address and specific UDP port numbers. The combination of the IP address and UDP port number creates a unique identifier, allowing different ports to be individually defined as RADIUS host entries providing a specific AAA service. If two different host entries on the same RADIUS server are configured for the same service—for example, accounting—the second host entry configured acts as failover backup to the first one. Using this

example, if the first host entry fails to provide accounting services, the network access server will try the second host entry configured on the same device for accounting services. (The RADIUS host entries will be tried in the order they are configured.)

Examples

Configuring Multiple Entries for the Same Server IP Address

The following example shows the network access server configured to recognize several RADIUS host entries with the same IP address. Two different host entries on the same RADIUS server are configured for the same services—authentication and accounting. The second host entry configured acts as fail-over backup to the first one. (The RADIUS host entries are tried in the order in which they are configured.)

```
! This command enables AAA.
aaa new-model
! The next command configures default RADIUS parameters.
aaa authentication ppp default radius
! The next set of commands configures multiple host entries for the same IP address.
radius-server host 172.20.0.1 auth-port 1000 acct-port 1001
radius-server host 172.20.0.1 auth-port 2000 acct-port 2000
```

Configuring Multiple Entries Using AAA Group Servers

In this example, the network access server is configured to recognize two different RADIUS group servers. One of these groups, group1, has two different host entries on the same RADIUS server configured for the same services. The second host entry configured acts as failover backup to the first one.

```
! This command enables AAA.
aaa new-model
! The next command configures default RADIUS parameters.
aaa authentication ppp default group group1
! The following commands define the group1 RADIUS group server and associates servers
! with it.
aaa group server radius group1
    server 172.20.0.1 auth-port 1000 acct-port 1001
! The following commands define the group2 RADIUS group server and associates servers
! with it.
aaa group server radius group2
    server 172.20.0.1 auth-port 2000 acct-port 2001
! The following set of commands configures the RADIUS attributes for each host entry
! associated with one of the defined group servers.
radius-server host 172.20.0.1 auth-port 1000 acct-port 1001
radius-server host 172.20.0.1 auth-port 1000 acct-port 1001
radius-server host 172.10.0.1 auth-port 1645 acct-port 1646
```

Related Commands

Command	Description
aaa group server	Groups different server hosts into distinct lists and distinct methods.
aaa new-model	Enables the AAA access control model.
radius-server host	Specifies a RADIUS server host.

server (TACACS+)

To configure the IP address of the TACACS+ server for the group server, use the **server** command in TACACS+ group server configuration mode. To remove the IP address of the RADIUS server, use the **no** form of this command.

server *ip-address*

no server *ip-address*

Syntax Description

<i>ip-address</i>	IP address of the selected server.
-------------------	------------------------------------

Defaults

No default behavior or values.

Command Modes

TACACS+ group server configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

You must configure the **aaa group server tacacs** command before configuring this command.

Enter the **server** command to specify the IP address of the TACACS+ server. Also configure a matching **tacacs-server host** entry in the global list. If there is no response from the first host entry, the next host entry is tried.

Examples

The following example shows server host entries configured for the RADIUS server:

```
aaa new-model
aaa authentication ppp default group g1
aaa group server tacacs+ g1
  server 1.0.0.1
  server 2.0.0.1
tacacs-server host 1.0.0.1
tacacs-server host 2.0.0.1
```

Related Commands

Command	Description
aaa new-model	Enables the AAA access control model.
aaa server group	Groups different server hosts into distinct lists and distinct methods.
tacacs-server host	Specifies a RADIUS server host.

server-private (RADIUS)

To configure the IP address of the private RADIUS server for the group server, use the **server-private** command in server-group configuration mode. To remove the associated private server from the authentication, authorization, and accounting (AAA) group server, use the **no** form of this command.

server-private *ip-address* [**auth-port** *port-number* | **acct-port** *port-number*] [**non-standard**] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*]

no server-private *ip-address* [**auth-port** *port-number* | **acct-port** *port-number*] [**non-standard**] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*]

Syntax Description

<i>ip-address</i>	IP address of the private RADIUS server host.
auth-port <i>port-number</i>	(Optional) User Datagram Protocol (UDP) destination port for authentication requests. The default value is 1645.
acct-port <i>port-number</i>	(Optional) UDP destination port for accounting requests. The default value is 1646.
non-standard	(Optional) RADIUS server is using vendor-proprietary RADIUS attributes.
timeout <i>seconds</i>	(Optional) Time interval (in seconds) that the router waits for the RADIUS server to reply before retransmitting. This setting overrides the global value of the radius-server timeout command. If no timeout value is specified, the global value is used.
retransmit <i>retries</i>	(Optional) Number of times a RADIUS request is resent to a server, if that server is not responding or responding slowly. This setting overrides the global setting of the radius-server retransmit command.
key <i>string</i>	(Optional) Authentication and encryption key used between the router and the RADIUS daemon running on the RADIUS server. This key overrides the global setting of the radius-server key command. If no key string is specified, the global value is used.

Defaults

If server-private parameters are not specified, global configurations will be used; if global configurations are not specified, default values will be used.

Command Modes

Server-group configuration

Command History

Release	Modification
12.2(1)DX	This command was introduced on the Cisco 7200 series and Cisco 7401ASR.
12.2(2)DD	This command was integrated into Cisco IOS Release 12.2(2)DD.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines

Use the **server-private** command to associate a particular private server with a defined server group. To prevent possible overlapping of private addresses between Virtual Route Forwardings (VRFs), private servers (servers with private addresses) can be defined within the server group and remain hidden from other groups, while the servers in the global pool (default “radius” server group) can still be referred to by IP addresses and port numbers. Thus, the list of servers in server groups includes references to the hosts in the global configuration and the definitions of private servers.

Examples

The following example shows how to define the sg_water RADIUS group server and associate private servers with it:

```
aaa group server radius sg_water
  server-private 10.1.1.1 timeout 5 retransmit 3 key coke
  server-private 10.2.2.2 timeout 5 retransmit 3 key coke
```

Related Commands

Command	Description
aaa group server	Groups different server hosts into distinct lists and distinct methods.
aaa new-model	Enables the AAA access control model.
radius-server host	Specifies a RADIUS server host.

service password-encryption

To encrypt passwords, use the **service password-encryption** command in global configuration mode. To restore the default, use the **no** form of this command.

service password-encryption

no service password-encryption

Syntax Description This command has no arguments or keywords.

Defaults No encryption

Command Modes Global configuration

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines The actual encryption process occurs when the current configuration is written or when a password is configured. Password encryption is applied to all passwords, including username passwords, authentication key passwords, the privileged command password, console and virtual terminal line access passwords, and Border Gateway Protocol neighbor passwords. This command is primarily useful for keeping unauthorized individuals from viewing your password in your configuration file.

When password encryption is enabled, the encrypted form of the passwords is displayed when a **more system:running-config** command is entered.



Caution

This command does not provide a high level of network security. If you use this command, you should also take additional network security measures.



Note

You cannot recover a lost encrypted password. You must clear NVRAM and set a new password.

Examples The following example causes password encryption to take place:

```
service password-encryption
```

Related Commands	Command	Description
	enable password	Sets a local password to control access to various privilege levels.
	key-string (authentication)	Specifies the authentication string for a key.
	neighbor password	Enables MD5 authentication on a TCP connection between two BGP peers.

set aggressive-mode client-endpoint

To specify the Tunnel-Client-Endpoint attribute within an Internet Security Association Key Management Protocol (ISAKMP) peer configuration, use the **set aggressive-mode client-endpoint** command in ISAKMP policy configuration mode. To remove this attribute from your configuration, use the **no** form of this command.

set aggressive-mode client-endpoint *client-endpoint*

no set aggressive-mode client-endpoint *client-endpoint*

Syntax Description	<i>client-endpoint</i>	<p>One of the following identification types of the initiator end of the tunnel:</p> <ul style="list-style-type: none"> • ID_IPV4 (IPv4 address) • ID_FQDN (fully qualified domain name, for example “foo.cisco.com”) • ID_USER_FQDN (e-mail address) <p>The ID type is translated to the corresponding ID type in Internet Key Exchange (IKE).</p>
---------------------------	------------------------	--

Defaults The Tunnel-Client-Endpoint attribute is not defined.

Command Modes ISAKMP policy configuration

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

Usage Guidelines Before you can use this command, you must enable the **crypto isakmp peer** command.

To initiate an IKE aggressive mode negotiation and specify the RADIUS Tunnel-Client-Endpoint attribute, the **set aggressive-mode client-endpoint** command, along with the **set aggressive-mode password** command, *must* be configured in the ISAKMP peer policy. The Tunnel-Client-Endpoint attribute will be communicated to the server by encoding it in the appropriate IKE identity payload.

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

```
crypto isakmp peer address 4.4.4.1
set aggressive-mode client-endpoint user-fqdn user@cisco.com
set aggressive-mode password cisco123
```

■ **set aggressive-mode client-endpoint**

Related Commands	Command	Description
	crypto isakmp peer	Enables an IPSec peer for IKE querying of AAA for tunnel attributes in aggressive mode.
	set aggressive-mode password	Specifies the Tunnel-Password attribute within an ISAKMP peer configuration.

set aggressive-mode password

To specify the Tunnel-Password attribute within an Internet Security Association Key Management Protocol (ISAKMP) peer configuration, use the **set aggressive-mode password** command in ISAKMP policy configuration mode. To remove this attribute from your configuration, use the **no** form of this command.

```
set aggressive-mode password password
```

```
no set aggressive-mode password password
```

Syntax Description	<i>password</i>	Password that is used to authenticate the peer to a remote server. The tunnel password is used as the Internet Key Exchange (IKE) preshared key.
---------------------------	-----------------	--

Defaults	The Tunnel-Password attribute is not defined.
-----------------	---

Command Modes	ISAKMP policy configuration
----------------------	-----------------------------

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

Usage Guidelines	<p>Before you can use this command, you must enable the crypto isakmp peer command.</p> <p>To initiate an IKE aggressive mode negotiation, the set aggressive-mode password command, along with the set aggressive-mode client-endpoint command, <i>must</i> be configured in the ISAKMP peer policy. The Tunnel-Password attribute will be used as the IKE preshared key for the aggressive mode negotiation.</p>
-------------------------	---

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

```
crypto isakmp peer address 4.4.4.1
set aggressive-mode client-endpoint user-fqdn user@cisco.com
set aggressive-mode password cisco123
```

Related Commands	Command	Description
	crypto isakmp peer	Enables an IPsec peer for 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 isakmp-profile

To set the Internet Security Association and Key Management Protocol (ISAKMP) profile name, use the **set isakmp-profile** command in crypto map configuration mode. To remove the ISAKMP profile name, use the **no** form of this command.

set isakmp-profile *profile-name*

no set isakmp-profile *profile-name*

Syntax Description

<i>profile-name</i>	Name of the ISAKMP profile.
---------------------	-----------------------------

Defaults

If the ISAKMP profile is not specified in the crypto map entry, the default is to the ISAKMP profile that is on the head. If there is no ISAKMP profile on the head, the default is “none.”

Command Modes

Crypto map configuration

Command History

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

Usage Guidelines

This command describes the ISAKMP profile to use when you start the Internet Key Exchange (IKE) exchange.

Before configuring an ISAKMP profile on a crypto map, you should set up the ISAKMP profile.

Examples

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

```
crypto map vpnmap 10 ipsec-isakmp
 set isakmp-profile vpnprofile
```

Related Commands

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

set peer (IPSec)

To specify an IP Security peer in a crypto map entry, use the **set peer** command in crypto map configuration mode. To remove an IPSec peer from a crypto map entry, use the **no** form of this command.

```
set peer {host-name | ip-address}
```

```
no set peer {host-name | ip-address}
```

Syntax Description

<i>host-name</i>	Specifies the IPSec peer by its host name. This is the peer's host name concatenated with its domain name (for example, myhost.example.com).
<i>ip-address</i>	Specifies the IPSec peer by its IP address.

Defaults

No peer is defined by default.

Command Modes

Crypto map configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

Use this command to specify an IPSec peer for a crypto map.

This command is required for all static crypto maps. If you are defining a dynamic crypto map (with the **crypto dynamic-map** command), this command is not required, and in most cases is not used (because, in general, the peer is unknown).

For **ipsec-isakmp** crypto map entries, you can specify multiple peers by repeating this command. The peer that packets are actually sent to is determined by the last peer that the router heard from (received either traffic or a negotiation request from) for a given data flow. If the attempt fails with the first peer, Internet Key Exchange tries the next peer on the crypto map list.

For **ipsec-manual** crypto entries, you can specify only one IPSec peer per crypto map. If you want to change the peer, you must first delete the old peer and then specify the new peer.

You can specify the remote IPSec peer by its host name only if the host name is mapped to the peer's IP address in a Domain Name Server or if you manually map the host name to the IP address with the **ip host** command.

Examples

The following example shows a crypto map configuration when IKE will be used to establish the security associations. In this example, a security association could be set up to either the IPSec peer at 10.0.0.1 or the peer at 10.0.0.2.

```
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
```

Related Commands	Command	Description
	crypto dynamic-map	Creates a dynamic crypto map entry and enters the crypto map configuration command mode.
	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 pfs	Specifies that IPSec should ask for 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 level per-host	Specifies that separate IPSec security associations 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 security associations.
	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.

set pfs

To specify that IP Security (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, use the **set pfs** command in crypto map configuration mode. To specify that IPSec should not request PFS, use the **no** form of this command.

```
set pfs [group1 | group2]
```

```
no set pfs
```

Syntax Description

group1	(Optional) Specifies that IPSec should use the 768-bit Diffie-Hellman prime modulus group when performing the new Diffie-Hellman exchange.
group2	(Optional) Specifies that IPSec should use the 1024-bit Diffie-Hellman prime modulus group when performing the new Diffie-Hellman exchange.

Defaults

By default, PFS is not requested. If no group is specified with this command, **group1** is used as the default.

Command Modes

Crypto map configuration

Command History

Release	Modification
11.3 T	This command was introduced.

Usage Guidelines

This command is only available for **ipsec-isakmp** crypto map entries and dynamic crypto map entries.

During negotiation, this command causes IPSec to request PFS when requesting new security associations for the crypto map entry. The default (**group1**) is sent if the **set pfs** statement does not specify a group. If the peer initiates the negotiation and the local configuration specifies PFS, the remote peer must perform a PFS exchange or the negotiation will fail. If the local configuration does not specify a group, a default of **group1** will be assumed, and an offer of either **group1** or **group2** will be accepted. If the local configuration specifies **group2**, that group *must* be part of the peer's offer or the negotiation will fail. If the local configuration does not specify PFS it will accept any offer of PFS from the peer.

PFS adds another level of security because if one key is ever cracked by an attacker then only the data sent with that key will be compromised. Without PFS, data sent with other keys could be also compromised.

With PFS, every time a new security association is negotiated, a new Diffie-Hellman exchange occurs. (This exchange requires additional processing time.)

The 1024-bit Diffie-Hellman prime modulus group, **group2**, provides more security than **group1**, but requires more processing time than **group1**.

Examples

The following example specifies that PFS should be used whenever a new security association is negotiated for the crypto map “mymap 10”:

```
crypto map mymap 10 ipsec-isakmp
  set pfs group2
```

Related Commands

Command	Description
crypto dynamic-map	Creates a dynamic crypto map entry and enters the crypto map configuration command mode.
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 security-association level per-host	Specifies that separate IPsec security associations 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 security associations.
set transform-set	Specifies which transform sets can be used with the crypto map entry.
show crypto map (IPsec)	Displays the crypto map configuration.

set security-association level per-host

To specify that separate IP Security security associations should be requested for each source/destination host pair, use the **set security-association level per-host** command in crypto map configuration mode. To specify that one security association should be requested for each crypto map access list **permit** entry, use the **no** form of this command.

set security-association level per-host

no set security-association level per-host

Syntax Description

This command has no arguments or keywords.

Defaults

For a given crypto map, all traffic between two IPSec peers matching a single crypto map access list **permit** entry will share the same security association.

Command Modes

Crypto map configuration

Command History

Release	Modification
11.3 T	This command was introduced.

Usage Guidelines

This command is only available for **ipsec-isakmp** crypto map entries and is not supported for dynamic crypto map entries.

When you use this command, you need to specify that a separate security association should be used for each source/destination host pair.

Normally, within a given crypto map, IPSec will attempt to request security associations at the granularity specified by the access list entry. For example, if the access list entry permits IP protocol traffic between subnet A and subnet B, IPSec will attempt to request security associations between subnet A and subnet B (for any IP protocol), and unless finer-grained security associations are established (by a peer request), all IPSec-protected traffic between these two subnets would use the same security association.

This command causes IPSec to request separate security associations for each source/destination host pair. In this case, each host pairing (where one host was in subnet A and the other host was in subnet B) would cause IPSec to request a separate security association.

With this command, one security association would be requested to protect traffic between host A and host B, and a different security association would be requested to protect traffic between host A and host C.

The access list entry can specify local and remote subnets, or it can specify a host-and-subnet combination. If the access list entry specifies protocols and ports, these values are applied when establishing the unique security associations.

Use this command with care, as multiple streams between given subnets can rapidly consume system resources.

Examples

The following example shows what happens with an access list entry of **permit ip 1.1.1.0 0.0.0.255 2.2.2.0 0.0.0.255** and a per-host level:

- A packet from 1.1.1.1 to 2.2.2.1 will initiate a security association request, which would look like it originated via **permit ip host 1.1.1.1 host 2.2.2.1**.
- A packet from 1.1.1.1 to 2.2.2.2 will initiate a security association request, which would look like it originated via **permit ip host 1.1.1.1 host 2.2.2.2**.
- A packet from 1.1.1.2 to 2.2.2.1 will initiate a security association request, which would look like it originated via **permit ip host 1.1.1.2 host 2.2.2.1**.

Without the per-host level, any of the above packets will initiate a single security association request originated via **permit ip 1.1.1.0 0.0.0.255 2.2.2.0 0.0.0.255**.

Related Commands

Command	Description
crypto dynamic-map	Creates a dynamic crypto map entry and enters the crypto map configuration command mode.
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 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 map (IPSec)	Displays the crypto map configuration.

set security-association lifetime

To override (for a particular crypto map entry) the global lifetime value, which is used when negotiating IP Security security associations, use the **set security-association lifetime** command in crypto map configuration mode. To reset a crypto map entry's lifetime value to the global value, use the **no** form of this command.

```
set security-association lifetime {seconds seconds | kilobytes kilobytes}
```

```
no set security-association lifetime {seconds | kilobytes}
```

Syntax Description

seconds <i>seconds</i>	Specifies the number of seconds a security association will live before expiring.
kilobytes <i>kilobytes</i>	Specifies the volume of traffic (in kilobytes) that can pass between IPSec peers using a given security association before that security association expires.

Defaults

The crypto map's security associations are negotiated according to the global lifetimes.

Command Modes

Crypto map configuration

Command History

Release	Modification
11.3 T	This command was introduced.

Usage Guidelines

This command is available only for **ipsec-isakmp** crypto map entries and dynamic crypto map entries. IPSec security associations use shared secret keys. These keys and their security associations time out together.

Assuming that the particular crypto map entry has lifetime values configured, when the router requests new security associations during security association negotiation, it will specify its crypto map 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 session keys/security association expires after the first of these lifetimes is reached.

If you change a lifetime, the change will not be applied to existing security associations, but will be used in subsequent negotiations to establish security associations for data flows supported by this crypto map entry. 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 detail.

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

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

Shorter lifetimes can make it harder to mount a successful key recovery attack, because the attacker has less data encrypted under the same key to work with. However, shorter lifetimes need more CPU processing time.

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

How These Lifetimes Work

Assuming that the particular crypto map entry does not have lifetime values configured, when the router requests new security associations it will specify its global lifetime values 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 either the lifetime value proposed by the peer or the locally configured lifetime value as the lifetime of the new security associations.

The security association (and corresponding keys) will expire according to whichever occurs sooner, either after the **seconds** time out or after the **kilobytes** amount of traffic is passed.

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 the timed lifetime for a particular crypto map entry, because there is a higher risk that the keys could be compromised for security associations belonging to the crypto map entry. The traffic-volume lifetime is not changed because there is not a high volume of traffic anticipated for these security associations. The timed lifetime is shortened to 2700 seconds (45 minutes).

```
crypto map mymap 10 ipsec-isakmp
 set security-association lifetime seconds 2700
```

Related Commands

Command	Description
crypto dynamic-map	Creates a dynamic crypto map entry and enters the crypto map configuration command mode.
crypto ipsec security-association lifetime	Changes global lifetime values used when negotiating IPSec security associations.
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.

Command	Description
set peer (IPSec)	Specifies an IPSec peer in a crypto map entry.
set pfs	Specifies that IPSec should ask for 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 level per-host	Specifies that separate IPSec security associations should be requested for each source/destination host pair.
set transform-set	Specifies which transform sets can be used with the crypto map entry.
show crypto map (IPSec)	Displays the crypto map configuration.

set session-key

To manually specify the IP Security session keys within a crypto map entry, use the **set session-key** command in crypto map configuration mode. This command is available only for **ipsec-manual** crypto map entries. To remove IPsec session keys from a crypto map entry, use the **no** form of this command.

Authentication Header (AH) Protocol Syntax

```
set session-key {inbound | outbound} ah spi hex-key-string
```

```
no set session-key {inbound | outbound} ah
```

Encapsulation Security Protocol (ESP) Syntax

```
set session-key {inbound | outbound} esp spi cipher hex-key-string
    [authenticator hex-key-string]
```

```
no set session-key {inbound | outbound} esp
```

Syntax Description	
inbound	Sets the inbound IPsec session key. (You must set both inbound and outbound keys.)
outbound	Sets the outbound IPsec session key. (You must set both inbound and outbound keys.)
ah	Sets the IPsec session key for the AH protocol. Use when the crypto map entry's transform set includes an AH transform.
esp	Sets the IPsec session key for ESP. Use when the crypto map entry's transform set includes an ESP transform.
<i>spi</i>	Specifies the security parameter index (SPI), a number that is used to uniquely identify a security association. The SPI is an arbitrary number you assign in the range of 256 to 4,294,967,295 (FFFF FFFF). You can assign the same SPI to both directions and both protocols. However, not all peers have the same flexibility in SPI assignment. For a given destination address/protocol combination, unique SPI values must be used. The destination address is that of the router if inbound, the peer if outbound.
<i>hex-key-string</i>	Specifies the session key; enter in hexadecimal format. This is an arbitrary hexadecimal string of 8, 16, or 20 bytes. If the crypto map's transform set includes a DES algorithm, specify at least 8 bytes per key. If the crypto map's transform set includes an MD5 algorithm, specify at least 16 bytes per key. If the crypto map's transform set includes an SHA algorithm, specify 20 bytes per key. Keys longer than the above sizes are simply truncated.
<i>cipher</i>	Indicates that the key string is to be used with the ESP encryption transform.
authenticator	(Optional) Indicates that the key string is to be used with the ESP authentication transform. This argument is required only when the crypto map entry's transform set includes an ESP authentication transform.

The following example shows a crypto map entry for manually established security associations. The transform set “someset” includes both an AH and an ESP protocol, so session keys are configured for both AH and ESP for both inbound and outbound traffic. The transform set includes both encryption and authentication ESP transforms, so session keys are created for both using the **cipher** and **authenticator** keywords.

```
crypto ipsec transform-set someset ah-sha-hmac esp-des esp-sha-hmac

crypto map mymap 10 ipsec-manual
 match address 101
 set transform-set someset
 set peer 10.0.0.1
 set session-key inbound ah 300 9876543210987654321098765432109876543210
 set session-key outbound ah 300 fedcbafedcbafedcbafedcbafedcbafedcbafedc
 set session-key inbound esp 300 cipher 0123456789012345
 authenticator 0000111122223333444455556666777788889999
 set session-key outbound esp 300 cipher abcdefabcdefabcd
 authenticator 9999888877776666555544443333222211110000
```

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 transform-set	Specifies which transform sets can be used with the crypto map entry.
show crypto map (IPSec)	Displays the crypto map configuration.

set transform-set

To specify which transform sets can be used with the crypto map entry, use the **set transform-set** command in crypto map configuration mode. To remove all transform sets from a crypto map entry, use the **no** form of this command.

```
set transform-set transform-set-name [transform-set-name2...transform-set-name6]
```

```
no set transform-set
```

Syntax Description

transform-set-name Name of the transform set.

For an **ipsec-manual** crypto map entry, you can specify only one transform set.

For an **ipsec-isakmp** or dynamic crypto map entry, you can specify up to six transform sets.

Defaults

No transform sets are included by default.

Command Modes

Crypto map configuration

Command History

Release	Modification
11.3 T	This command was introduced.

Usage Guidelines

This command is required for all static and dynamic crypto map entries.

Use this command to specify which transform sets to include in a crypto map entry.

For an **ipsec-isakmp** crypto map entry, you can list multiple transform sets with this command. List the higher priority transform sets first.

If the local router initiates the negotiation, the transform sets are presented to the peer in the order specified in the crypto map entry. If the peer initiates the negotiation, the local router accepts the first transform set that matches one of the transform sets specified in the crypto map entry.

The first matching transform set that is found at both peers is used for the security association. If no match is found, IPsec will not establish a security association. The traffic will be dropped because there is no security association to protect the traffic.

For an **ipsec-manual** crypto map entry, you can specify only one transform set. If the transform set does not match the transform set at the remote peer's crypto map, the two peers will fail to correctly communicate because the peers are using different rules to process the traffic.

If you want to change the list of transform sets, re-specify the new list of transform sets to replace the old list. This change is only applied to crypto map entries that reference this transform set. 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.

Any transform sets included in a crypto map must previously have been defined using the **crypto ipsec transform-set** command.

Examples

The following example defines two transform sets and specifies that they can both be used within a crypto map entry. (This example applies only when IKE is used to establish security associations. With crypto maps used for manually established security associations, only one transform set can be included in a given crypto map entry.)

```
crypto ipsec transform-set my_t_set1 esp-des esp-sha-hmac
crypto ipsec transform-set my_t_set2 ah-sha-hmac esp-des esp-sha-hmac

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

In this example, when traffic matches access list 101, the security association can use either transform set “my_t_set1” (first priority) or “my_t_set2” (second priority) depending on which transform set matches the remote peer’s transform sets.

show aaa attributes

To display the mapping between an authentication, authorization, and accounting (AAA) attribute number and the corresponding AAA attribute name, use the **show aaa attributes** command in EXEC configuration mode.

```
show aaa attributes [protocol radius]
```

Syntax Description

protocol radius	(Optional) Displays the mapping between a RADIUS attribute and a AAA attribute name and number.
------------------------	---

Command Modes

EXEC

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.2(11)T	The protocol and radius keywords were added.

Examples

The following example is sample output for the **show aaa attributes** command. In this example, all RADIUS attributes that have been enabled are displayed.

```
Router# show aaa attributes protocol radius
```

```
AAA ATTRIBUTE LIST:
  Type=1      Name=disc-cause-ext          Format=Enum
  Protocol:RADIUS
  Non-Standard Type=195 Name=Ascend-Disconnect-Cau Format=Enum
  Cisco VSA   Type=1      Name=Cisco AVpair      Format=String
  Type=2      Name=Acct-Status-Type          Format=Enum
  Protocol:RADIUS
  IETF        Type=40     Name=Acct-Status-Type  Format=Enum
  Type=3      Name=acl                          Format=Ulong
  Protocol:RADIUS
  IETF        Type=11     Name=Filter-Id         Format=Binary
  Type=4      Name=addr                          Format=IPv4 Address
  Protocol:RADIUS
  IETF        Type=8      Name=Framed-IP-Address Format=IPv4 Address
  Type=5      Name=addr-pool                     Format=String
  Protocol:RADIUS
  Non-Standard Type=218 Name=Ascend-IP-Pool    Format=Ulong
  Type=6      Name=asyncmap                       Format=Ulong
  Protocol:RADIUS
  Non-Standard Type=212 Name=Ascend-Asyncmap   Format=Ulong
  Type=7      Name=Authentic                      Format=Enum
  Protocol:RADIUS
  IETF        Type=45     Name=Authentic         Format=Enum
  Type=8      Name=autocmd                       Format=String
```

show aaa cache filterserver

To display the cache status, use the **show aaa cache filterserver** command in EXEC mode.

show aaa cache filterserver

Syntax Description This command has no arguments or keywords.

Command Modes EXEC

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

Usage Guidelines The **show aaa cache filterserver** command shows how many times a particular filter has been referenced or refreshed. This function may be used in administration to determine which filters are actually being used.

Examples The following is sample output for the **show aaa cache filterserver** command:

```
Router# show aaa cache filterserver
```

```
Filter      Server      Age Expires Refresh Access-Control-Lists
-----
aol         1.2.3.4      0   1440   100 ip in icmp drop
           ip out icmp drop
           ip out forward tcp dstip 1.2.3...
msn         1.2.3.4      N/A Never    2 ip in tcp drop
msn2        1.2.3.4      N/A Never    2 ip in tcp drop
vone        1.2.3.4      N/A Never    0 ip in tcp drop
```

[Table 22](#) describes the significant fields shown in the display.

Table 22 *show aaa cache filterserver Field Descriptions*

Field	Description
Filter	Filter name.
Server	RADIUS server IP address.
Age	When to expire a cache entry.
Expires	Number of minutes in which a cache entry will expire.
Refresh	Number of times a cache has been refreshed.
Access-Control-Lists	Access control list (ACL) of the server.

Related Commands

Command	Description
aaa authorization cache filterserver	Enables AAA authorization caches and the downloading of ACL configurations from a RADIUS filter server.

show aaa server-private

To display the status of all private RADIUS servers, use the **show aaa server-private** command in EXEC mode.

show aaa server-private

Syntax Description This command has no arguments or keywords.

Command Modes User and privileged EXEC

Command History	Release	Modification
	12.3	This command was introduced.

Examples The following is sample output from the **show aaa server-private** command. Only the first four lines of the display pertain to the status of private RADIUS servers, and the fields in this part of the display are described in [Table 23](#).

```
Router# show aaa server-private

RADIUS: id 24, priority 1, host 172.31.164.120, auth-port 1645,
acct-port 1646
  State: current UP, duration 18s, previous duration 0s
  Dead: total time 0s, count 0
  Authen: request 0, timeouts 0
          Response: unexpected 0, server error 0, incorrect 0, time 0ms
          Transaction: success 0, failure 0
  Author: request 0, timeouts 0
          Response: unexpected 0, server error 0, incorrect 0, time 0ms
          Transaction: success 0, failure 0
  Account: request 0, timeouts 0
           Response: unexpected 0, server error 0, incorrect 0, time 0ms
           Transaction: success 0, failure 0
  Elapsed time since counters last cleared: 2h1m
```

Table 23 show aaa server-private Command Field Descriptions

Field	Description
id	A unique identifier for all AAA servers defined on the router.
priority	The order of use for servers within a group.
host	IP address of the private RADIUS server host.
auth-port	User Datagram Protocol (UDP) destination port for authentication requests. The default value is 1645.
acct-port	UDP destination port for accounting requests. The default value is 1646.

Table 23 *show aaa server-private Command Field Descriptions (continued)*

Field	Description
State:	Describes the current state of the server, how long, in seconds, the server has been in that state, and how long, in seconds, it was in the Previous state.
Dead:	Indicates the number of times that this server has been marked dead and the cumulative amount of time, in seconds, that it spent in that state.

Related Commands

Command	Description
server-private	Associates a particular private RADIUS server with a defined server group.

show aaa user

To display attributes related to an authentication, authorization, and accounting (AAA) session, use the **show aaa user** command in privileged EXEC mode.

```
show aaa user {all | unique id}
```

Syntax Description

all	Displays information about all users for which AAA currently has knowledge.
<i>unique id</i>	Displays information for only this user.

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

When a user logs into a Cisco router and uses AAA, a unique ID is assigned to the session. Throughout the life of the session, various attributes that are related to the session are collected and stored internally within a AAA database. These attributes can include the IP address of the user, the protocol being used to access the router (such as PPP or Serial Line Internet Protocol [SLIP]), the speed of the connection, and the number of packets or bytes that are received or transmitted.

The output of this command provides a snapshot of various subdatabases that are associated with a AAA unique ID. Some of the more important ones are listed in [Table 24](#).

The output also shows various AAA call events that are associated with a particular session. For example, when a session comes up, the events generally recorded are CALL START, NET UP, and IP Control Protocol UP (IPCP UP).

In addition, the output provides a snapshot of the dynamic attributes that are associated with a particular session. (Dynamic attributes are those that keep changing values throughout the life of the session.) Some of the more important ones are listed in [Table 24](#).

The unique ID of a session can be obtained from the output of the **show aaa sessions** command.



Note This command does not provide information for all users who are logged into a device, but for only those who have been authenticated or authorized using AAA or for only those whose sessions are being accounted for by the AAA module.



Note Using the **all** keyword can produce a large amount of output, depending on the number of users who are logged into the device at any given time.

Examples

The following example shows that information is requested for all users:

```
Router# show aaa user all
```

The following example shows that information is requested for user 5:

```
Router# show aaa user 5
```

The following is sample output from the **show aaa user** command. The session information displayed is for a PPP over Ethernet over Ethernet (PPPoEoE) session.

```
Router# show aaa user 3
```

```
Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
Time source is hardware calendar, *20:32:49.199 PST Wed Dec 17
2003
```

```
Unique id 3 is currently in use.
```

```
Accounting:
```

```
log=0x20C201
```

```
Events recorded :
```

```
CALL START
```

```
NET UP
```

```
IPCP_PASS
```

```
INTERIM START
```

```
VPDN NET UP
```

```
update method(s) :
```

```
NONE
```

```
update interval = 0
```

```
Outstanding Stop Records : 0
```

```
Dynamic attribute list:
```

```
63CCF138 0 00000001 connect-progress(30) 4 LAN Ses Up
```

```
63CCF14C 0 00000001 pre-session-time(239) 4 3(3)
```

```
63CCF160 0 00000001 nas-tx-speed(337) 4 102400000(61A8000)
```

```
63CCF174 0 00000001 nas-rx-speed(33) 4 102400000(61A8000)
```

```
63CCF188 0 00000001 elapsed_time(296) 4 2205(89D)
```

```
63CCF19C 0 00000001 bytes_in(97) 4 6072(17B8)
```

```
63CCF1B0 0 00000001 bytes_out(223) 4 6072(17B8)
```

```
63CCF1C4 0 00000001 pre-bytes-in(235) 4 86(56)
```

```
63CCF1D8 0 00000001 pre-bytes-out(236) 4 90(5A)
```

```
63CCF1EC 0 00000001 paks_in(98) 4 434(1B2)
```

```
63CCF244 0 00000001 paks_out(224) 4 434(1B2)
```

```
63CCF258 0 00000001 pre-paks-in(237) 4 7(7)
```

```
63CCF26C 0 00000001 pre-paks-out(238) 4 9(9)
```

```
No data for type EXEC
```

```
No data for type CONN
```

```
NET: Username=peer1
```

```
Session Id=00000003 Unique Id=00000003
```

```
Start Sent=1 Stop Only=N
```

```
stop_has_been_sent=N
```

```
Method List=63B4A10C : Name = default
```

```
Attribute list:
```

```
63CCF138 0 00000001 session-id(293) 4 3(3)
```

```
63CCF14C 0 00000001 Framed-Protocol(62) 4 PPP
```

```
63CCF160 0 00000001 protocol(241) 4 ip
```

```
63CCF174 0 00000001 addr(5) 4 70.0.0.1
```

```
No data for type CMD
```

```
No data for type SYSTEM
```

```
No data for type RM CALL
```

```
No data for type RM VPDN
```

```
No data for type AUTH PROXY
```

```
No data for type IPSEC-TUNNEL
```

```
No data for type RESOURCE
```

```
No data for type 10
```

```

No data for type CALL
Debg: No data available
Radi: 641AACAC
Interface:
  TY Num = -1
  Stop Received = 0
  Byte/Packet Counts till Call Start:
    Start Bytes In = 106      Start Bytes Out = 168
    Start Paks   In = 3       Start Paks   Out = 4
  Byte/Packet Counts till Service Up:
    Pre Bytes In = 192       Pre Bytes Out = 258
    Pre Paks   In = 10       Pre Paks   Out = 13
  Cumulative Byte/Packet Counts :
    Bytes In = 6264          Bytes Out = 6330
    Paks   In = 444          Paks   Out = 447
  StartTime = 19:56:01 PST Dec 17 2003
  AuthenTime = 19:56:04 PST Dec 17 2003
  Component = PpOE
Authen: service=PPP type=CHAP method=RADIUS
Kerb: No data available
Meth: No data available
Preauth: No Preauth data.
General:
  Unique Id = 00000003
  Session Id = 00000003
  Attribute List:
    63CCF180 0 00000001 port-type(156) 4 PPP over Ethernet
    63CCF194 0 00000009 interface(152) 7 0/0/0/0
PerU: No data available

```

Table 24 lists the significant fields shown in the display.

Table 24 show aaa user Field Descriptions

Field	Description
EXEC	Exec-Accounting database
NET	Network Accounting database
CMD	Command Accounting database
Pre Bytes In	Bytes that were received before the call was authenticated
Pre Bytes Out	Bytes that were transmitted before the call was authenticated
Pre Paks In	Packets that were received before the call was authenticated
Pre Paks Out	Packets that were transmitted before the call was authenticated
Bytes In	Bytes that were received after the call was authenticated
Bytes Out	Bytes that were transmitted after the call was authenticated
Paks In	Packets that were received after the call was authenticated
Paks Out	Packets that were transmitted after the call was authenticated

Field	Description
Authen	Authentication database
General	General database
PerU	Per-User database

Related Commands

Command	Description
show aaa sessions	Displays information about AAA sessions as seen in the AAA Session MIB.

show accounting

The **show accounting** command is replaced by the **show aaa user** command. See the **show aaa user** command for more information.

show auto secure config

To display AutoSecure configurations, use the **show auto secure config** command in privileged EXEC mode.

show auto secure config

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.3(1)	This command was introduced.
	12.3(15)	Autosecure disables the configuration of the <code>autosec_iana_reserved_block</code> , <code>autosec_private_block</code> , or <code>autosec_complete_bogon</code> access control lists (acls), and application-to-edge interfaces. Output for these acls is no longer shown in the show output.
	12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.

Examples The following sample output from the **show auto secure config** command shows what has been enabled and disabled via the **auto secure** command:

```
Router# show auto secure config

no service finger
no service pad
no service udp-small-servers
no service tcp-small-servers
service password-encryption
service tcp-keepalives-in
service tcp-keepalives-out
no cdp run
no ip bootp server
no ip http server
no ip finger
no ip source-route
no ip gratuitous-arps
no ip identd
security passwords min-length 6
security authentication failure rate 10 log
enable secret 5 $1$CZ6G$GkGOnHdNJCO3CjNHHyTUA.
aaa new-model
aaa authentication login local_auth local
line console 0
  login authentication local_auth
  exec-timeout 5 0
  transport output telnet
line aux 0
  login authentication local_auth
  exec-timeout 10 0
  transport output telnet
```

```
line vty 0 4
  login authentication local_auth
  transport input telnet
ip domain-name cisco.com

crypto key generate rsa general-keys modulus 1024
ip ssh time-out 60
ip ssh authentication-retries 2
line vty 0 4
  transport input ssh telnet
service timestamps debug datetime localtime show-timezone msec
service timestamps log datetime localtime show-timezone msec
logging facility local2
logging trap debugging
service sequence-numbers
logging console critical
logging buffered
interface FastEthernet0/1
  no ip redirects
  no ip proxy-arp
  no ip unreachable
  no ip directed-broadcast
  no ip mask-reply
  no mop enabled
!
interface FastEthernet1/0
  no ip redirects
  no ip proxy-arp
  no ip unreachable
  no ip directed-broadcast
  no ip mask-reply
  no mop enabled
!
interface FastEthernet1/1
  no ip redirects
  no ip proxy-arp
  no ip unreachable
  no ip directed-broadcast
  no ip mask-reply
  no mop enabled
!
interface FastEthernet0/0
  no ip redirects
  no ip proxy-arp
  no ip unreachable
  no ip directed-broadcast
  no ip mask-reply
  no mop enabled
!
ip cef
interface FastEthernet0/0
  ip verify unicast reverse-path
ip inspect audit-trail
ip inspect dns-timeout 7
ip inspect tcp idle-time 14400
ip inspect udp idle-time 1800
ip inspect name autosec_inspect cuseeme timeout 3600
ip inspect name autosec_inspect ftp timeout 3600
ip inspect name autosec_inspect http timeout 3600
ip inspect name autosec_inspect rcmd timeout 3600
ip inspect name autosec_inspect realaudio timeout 3600
ip inspect name autosec_inspect smtp timeout 3600
ip inspect name autosec_inspect tftp timeout 30
ip inspect name autosec_inspect udp timeout 15
```

```
ip inspect name autosec_inspect tcp timeout 3600
access-list 100 deny ip any any
interface FastEthernet0/0
 ip inspect autosec_inspect out
 ip access-group 100 in
```

Related Commands

Command	Description
auto secure	Secures the management and forwarding planes of the router.

show crypto ca certificates

To display information about your certificate, the certification authority certificate, and any registration authority certificates, use the **show crypto ca certificates** command in EXEC mode.

show crypto ca certificates

Syntax Description This command has no arguments or keywords.

Command Modes EXEC

Command History	Release	Modification
	11.3 T	This command was introduced.

Usage Guidelines This command shows information about the following certificates:

- Your certificate, if you have requested one from the CA (see the **crypto ca enroll** command)
- The certificate of the CA, if you have received the CA's certificate (see the **crypto ca authenticate** command)
- RA certificates, if you have received RA certificates (see the **crypto ca authenticate** command)

Examples The following is sample output from the **show crypto ca certificates** command after you authenticated the CA by requesting the CA's certificate and public key with the **crypto ca authenticate** command:

```
CA Certificate
  Status: Available
  Certificate Serial Number: 3051DF7123BEE31B8341DFE4B3A338E5F
  Key Usage: Not Set
```

The CA certificate might show Key Usage as "Not Set."

The following is sample output from the **show crypto ca certificates** command, and shows the router's certificate and the CA's certificate. In this example, a single, general purpose RSA key pair was previously generated, and a certificate was requested but not received for that key pair.

```
Certificate
  Subject Name
    Name: myrouter.example.com
    IP Address: 10.0.0.1
    Serial Number: 04806682
  Status: Pending
  Key Usage: General Purpose
  Fingerprint: 428125BD A3419600 3F6C7831 6CD8FA95 00000000

CA Certificate
  Status: Available
  Certificate Serial Number: 3051DF7123BEE31B8341DFE4B3A338E5F
  Key Usage: Not Set
```

Note that in the previous sample, the router's certificate Status shows "Pending." After the router receives its certificate from the CA, the Status field changes to "Available" in the **show** output.

The following is sample output from the **show crypto ca certificates** command, and shows two router's certificates and the CA's certificate. In this example, special usage RSA key pairs were previously generated, and a certificate was requested and received for each key pair.

```
Certificate
  Subject Name
    Name: myrouter.example.com
    IP Address: 10.0.0.1
  Status: Available
  Certificate Serial Number: 428125BDA34196003F6C78316CD8FA95
  Key Usage: Signature
```

```
Certificate
  Subject Name
    Name: myrouter.example.com
    IP Address: 10.0.0.1
  Status: Available
  Certificate Serial Number: AB352356AFCD0395E333CCFD7CD33897
  Key Usage: Encryption
```

```
CA Certificate
  Status: Available
  Certificate Serial Number: 3051DF7123BEE31B8341DFE4B3A338E5F
  Key Usage: Not Set
```

The following is sample output from the **show crypto ca certificates** command when the CA supports an RA. In this example, the CA and RA certificates were previously requested with the **crypto ca authenticate** command.

```
CA Certificate
  Status: Available
  Certificate Serial Number: 3051DF7123BEE31B8341DFE4B3A338E5F
  Key Usage: Not Set
```

```
RA Signature Certificate
  Status: Available
  Certificate Serial Number: 34BCF8A0
  Key Usage: Signature
```

```
RA KeyEncipher Certificate
  Status: Available
  Certificate Serial Number: 34BCF89F
  Key Usage: Encryption
```

Related Commands

Command	Description
crypto ca authenticate	Authenticates the CA (by obtaining the certificate of the CA).
crypto ca enroll	Obtains the certificates of your router from the CA.
debug crypto pki messages	Displays debug messages for the details of the interaction (message dump) between the CA and the route.
debug crypto pki transactions	Displays debug messages for the trace of interaction (message type) between the CA and the router.

show crypto ca crls

To display the current certificate revocation list (CRL) on router, use the **show crypto ca crls** command in EXEC mode.

```
show crypto ca crls
```

Syntax Description This command has no arguments or keywords.

Command Modes EXEC

Command History	Release	Modification
	12.1	This command was introduced.

Examples The following is sample output of the **show crypto ca crls** command:

```
Router# show crypto ca crls

CRL Issuer Name:
OU = sjvpn, O = cisco, C = us
LastUpdate: 16:17:34 PST Jan 10 2002
NextUpdate: 17:17:34 PST Jan 11 2002
Retrieved from CRL Distribution Point:
LDAP: CN = CRL1, OU = sjvpn, O = cisco, C = us
```

Related Commands	Command	Description
	crypto ca crl request	Requests that a new CRL be obtained immediately from the CA.

show crypto ca roots

The **show crypto ca roots** command is replaced by the **show crypto ca trustpoints** command. See the **show crypto ca trustpoints** command for more information.

show crypto ca timers

To display the status of the managed timers that are maintained by Cisco IOS for public key infrastructure (PKI), use the **show crypto ca timers** command in EXEC mode.

show crypto ca timers

Syntax Description This command has no arguments or keywords.

Command Modes EXEC

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

Usage Guidelines For each timer, this command displays the time remaining before the timer expires. It also associates trustpoint certification authorities (CAs), except for certificate revocation list (CRL) timers, by displaying the CRL distribution point.

Examples The following example is sample output for the **show crypto ca timers** command:

```
Router# show crypto ca timers

PKI Timers
| 4d15:13:33.144
| 4d15:13:33.144 CRL http://msca-root.cisco.com/CertEnroll/msca-root.crl
| 328d11:56:48.372 RENEW msroot
| 6:43.201 POLL verisign
```

Related Commands	Command	Description
	auto-enroll	Enables autoenrollment.
	crypto ca trustpoint	Declares the CA that your router should use.

show crypto ca trustpoints

To display the trustpoints that are configured in the router, use the **show crypto ca trustpoints** command in EXEC mode.

show crypto ca trustpoints

Syntax Description This command has no arguments or keywords.

Command Modes EXEC

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

Usage Guidelines This command deprecates the **show crypto ca roots** command. If you enter the **show crypto ca roots** command, the output will be written back as the **show crypto ca trustpoints** command.

Examples The following is sample output from the **show crypto ca trustpoints** command:

```
Router# show crypto ca trustpoints

Trustpoint bo:
  Subject Name:
    CN = bomborra Certificate Manager
    O = cisco.com
    C = US
    Serial Number:01
  Certificate configured.
  CEP URL:http://bomborra
  CRL query url:ldap://bomborra
```

Related Commands	Command	Description
	crypto ca trustpoint	Declares the CA that your router should use.

show crypto dynamic-map

To display a dynamic crypto map set, use the **show crypto dynamic-map** command in EXEC mode.

```
show crypto dynamic-map [tag map-name]
```

Syntax Description	tag map-name (Optional) Displays only the crypto dynamic map set with the specified <i>map-name</i> .
---------------------------	--

Command Modes	EXEC
----------------------	------

Command History	Release	Modification
	11.3 T	This command was introduced.

Usage Guidelines Use the **show crypto dynamic-map** command to view a dynamic crypto map set.

Examples The following is sample output for the **show crypto dynamic-map** command:

```
Router# show crypto dynamic-map

Crypto Map Template"vpn1" 1
  ISAKMP Profile: vpn1-ra
  No matching address list set.
  Security association lifetime: 4608000 kilobytes/3600 seconds
  PFS (Y/N): N
  Transform sets={
    vpn1,
```

The following partial configuration was in effect when the above **show crypto dynamic-map** command was issued:

```
crypto dynamic-map vpn1 1
  set transform-set vpn1
  set isakmp-profile vpn1-ra
  reverse-route
```

Related Commands	Command	Description
	show crypto map	Views the crypto map configuration.

show crypto eng qos

To monitor and maintain low latency queueing (LLQ) for IP security (IPsec) encryption engines, use the **show crypto eng qos** command in privileged EXEC mode.

show crypto eng qos

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(13)T	This command was introduced.
	12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.

Usage Guidelines Use the **show crypto eng qos** command to determine whether quality of service (QoS) is enabled on LLQ for IPsec encryption engines.

Examples The following example shows whether LLQ for IPsec encryption engines is enabled:

```
Router# show crypto eng qos

crypto engine name: Multi-ISA Using VAM2
  crypto engine type: hardware
    slot: 5
    queuing: enabled
  visible bandwidth: 30000 kbps
    llq size: 0
  default queue size/max: 0/64
  interface table size: 32

  FastEthernet0/0 (3), iftype 1, ctable size 16, input filter:ip
  precedence 5
  class voice (1/3), match ip precedence 5
    bandwidth 500 kbps, max token 100000
    IN match pkt/byte 0/0, police drop 0
    OUT match pkt/byte 0/0, police drop 0

  class default, match pkt/byte 0/0, qdrop 0
  crypto engine bandwidth:total 30000 kbps, allocated 500 kbps
```

The field descriptions in the above display are self-explanatory.

show crypto engine accelerator logs

To display information about the last 32 CryptoGraphics eXtensions (CGX) Library packet processing commands and associated parameters sent from the VPN module driver to the VPN module hardware, use the **show crypto engine accelerator logs** command in privileged EXEC mode.

show crypto engine accelerator logs

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(1)XC	This command was introduced on the Cisco 1720 and Cisco 1750 platforms.
	12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.

Usage Guidelines Use this command when encrypted traffic is sent to the router and a problem with the encryption module is suspected. Use the **debug crypto engine accelerator logs** command to enable command logging *before* using this command.



Note

The **show crypto engine accelerator logs** command is intended only for Cisco Systems TAC personnel to collect debugging information.

Examples The following is sample output for the **show crypto engine accelerator logs** command:

```
Router# show crypto engine accelerator logs

Contents of packet log (current index = 20):

tag = 0x5B02, cmd = 0x5000
param[0] = 0x000E, param[1] = 0x57E8
param[2] = 0x0008, param[3] = 0x0000
param[4] = 0x0078, param[5] = 0x0004
param[6] = 0x142C, param[7] = 0x142C
param[8] = 0x0078, param[9] = 0x000C
tag = 0x5B03, cmd = 0x4100
param[0] = 0x000E, param[1] = 0x583C
param[2] = 0x0034, param[3] = 0x0040
param[4] = 0x00B0, param[5] = 0x0004
param[6] = 0x1400, param[7] = 0x1400
param[8] = 0x0020, param[9] = 0x000C
tag = 0x5C00, cmd = 0x4100
param[0] = 0x000E, param[1] = 0x57BC
param[2] = 0x0034, param[3] = 0x0040
param[4] = 0x00B0, param[5] = 0x0004
param[6] = 0x1400, param[7] = 0x1400
param[8] = 0x0020, param[9] = 0x000C
```

```

.
.
.
tag = 0x5A01, cmd = 0x4100
param[0] = 0x000E, param[1] = 0x593C
param[2] = 0x0034, param[3] = 0x0040
param[4] = 0x00B0, param[5] = 0x0004
param[6] = 0x1400, param[7] = 0x1400
param[8] = 0x0020, param[9] = 0x000C

Contents of cgx log (current index = 12):

cmd = 0x0074 ret = 0x0000
param[0] = 0x0010, param[1] = 0x028E
param[2] = 0x0039, param[3] = 0x0D1E
param[4] = 0x0100, param[5] = 0x0000
param[6] = 0x0000, param[7] = 0x0000
param[8] = 0x0000, param[9] = 0x0000
cmd = 0x0062 ret = 0x0000
param[0] = 0x0035, param[1] = 0x1BE0
param[2] = 0x0100, param[3] = 0x0222
param[4] = 0x0258, param[5] = 0x0000
param[6] = 0x0000, param[7] = 0x0000
param[8] = 0x0000, param[9] = 0x0000
cmd = 0x0063 ret = 0x0000
param[0] = 0x0222, param[1] = 0x0258
param[2] = 0x0000, param[3] = 0x0000
param[4] = 0x0000, param[5] = 0x0000
param[6] = 0x0000, param[7] = 0x020A
param[8] = 0x002D, param[9] = 0x0000
.
.
.
cmd = 0x0065 ret = 0x0000
param[0] = 0x0222, param[1] = 0x0258
param[2] = 0x0010, param[3] = 0x028E
param[4] = 0x00A0, param[5] = 0x0008
param[6] = 0x0001, param[7] = 0x0000
param[8] = 0x0000, param[9] = 0x0000

```

Related Commands

Command	Description
debug crypto engine accelerator logs	Enables logging of commands and associated parameters sent from the VPN module driver to the VPN module hardware using a debug flag.

show crypto engine accelerator ring

To display the contents and status of the control command, transmit packets, and receive packet rings used by the hardware accelerator crypto engine, use the **show crypto engine accelerator ring** command in privileged EXEC mode.

show crypto engine accelerator ring [control | packet | pool]

Syntax Description

control	(Optional) Number of control commands that are queued for execution by the hardware accelerator crypto engine are displayed.
packet	(Optional) Contents and status information for the transmit packet rings that are used by the hardware accelerator crypto engine are displayed.
pool	(Optional) Contents and status information for the receive packet rings that are used by the hardware accelerator crypto engine are displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(3)XL	This command was introduced 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 displays the command ring information.

If there were valid data in any of the rings, the ring entry would be printed.

Examples

The following example shows the command ring information:

```
Router# show crypto engine accelerator ring packet
```

```
PPQ RING:
```

```
cmd ring:head = 10 tail =10
```

```
result ring:head = 10 tail =10
```

```
destination ring:head = 10 tail =10
```

```
source ring:head = 10 tail =10
```

```

free ring:head = 0 tail =255
      00000000  071A96C5
      00000000  071A96C5
      00000001  071A9465
      00000001  071A9465
      00000002  071A9205
      00000002  071A9205
.
.
.

```

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 engine accelerator	Enables the use of the onboard hardware accelerator for IPSec encryption.
crypto ipsec	Defines the IPSec SAs 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 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.

show crypto engine accelerator sa-database

To display active (in-use) entries in the platform-specific virtual private network (VPN) module database, use the **show crypto engine accelerator sa-database** command in privileged EXEC mode.

show crypto engine accelerator sa-database

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(1)XC	This command was introduced on the Cisco 1720 and Cisco 1750 platforms.
	12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.

Usage Guidelines Use this command when encrypted traffic is sent to the router and a problem with the encryption module is suspected.



Note

The **show crypto engine accelerator sa-database** command is intended only for Cisco Systems TAC personnel to collect debugging information.

Examples The following is sample output for the **show crypto engine accelerator sa-database** command:

```
Router# show crypto engine accelerator sa-database

Flow Summary
  Index   Algorithms
  005     tunnel inbound esp-md5-hmac esp-des ah-sha-hmac
  006     tunnel outbound esp-md5-hmac esp-des ah-sha-hmac
  007     tunnel inbound esp-md5-hmac esp-des ah-sha-hmac
  008     tunnel outbound esp-md5-hmac esp-des ah-sha-hmac
  009     tunnel inbound esp-md5-hmac esp-des ah-sha-hmac
  010     tunnel outbound esp-md5-hmac esp-des ah-sha-hmac

SA Summary:
  Index   DH-Index   Algorithms
  003     001(deleted) DES SHA
  004     002(deleted) DES SHA

DH Summary
  Index Group Config
```

Related Commands	Command	Description
	debug crypto engine acclerator logs	Enables logging of commands and associated parameters sent from the VPN module driver to the VPN module hardware using a debug flag.

show crypto engine accelerator statistic

To display the statistics and error counters for the onboard hardware accelerator of the router for IP Security (IPSec) encryption, use the **show crypto engine accelerator statistic** command in privileged EXEC mode.

show crypto engine accelerator statistic

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(1)XC	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	This command was implemented on 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. In addition, the show output for this command was enhanced to display compression statistics.

Examples The following example displays compression statistics:

```
Router# show crypto engine accelerator statistic

Statistics for Hardware VPN Module:
  ds: 8235C3D8      idb: 82359A64
Statistics for Encryption Module:
  0 packets in 0 packets out
  0 packet overruns 0 output packets dropped
  0 packets decompressed 0 packets compressed
  0 compressed bytes in 0 encompassed bytes in
  0 packets bypass compression 0 packet abort compression
  0 packets fail compression
4:1 compression ratio 2:1 overall compression ratio
  0 decompressed bytes out 0 compressed bytes out
  0 packets decrypted 0 packets encrypted
  0 bytes decrypted 0 bytes encrypted
  0 bytes before decrypt 0 bytes after encrypt
  0 paks/sec in 0 paks/sec out
  0 Kbits/sec decrypted 0 Kbits/sec encrypted
  0 packet overruns
rx_no_endp:      0   rx_hi_discards:  0   fw_failure:      0
invalid_sa:      0   invalid_flow:    0   cgx_errors       0
fw_qs_filled:    0   fw_resource_lock:0   lotx_full_err:   0
null_ip_error:   0   pad_size_error:  0   out_bound_dh_acc:0
esp_auth_fail:   0   ah_auth_failure:0   crypto_pad_error:0
ah_prot_absent:  0   ah_seq_failure:  0   ah_spi_failure:  0
```

show crypto engine accelerator statistic

```

esp_prot_absent:0   esp_seq_fail:    0   esp_spi_failure:  0
obound_sa_acc:  0   invalid_sa:     0   out_bound_sa_flow: 0
invalid_dh:     0   bad_keygroup:  0   out_of_memory:    0
no_sh_secret:   0   no_keys:       0   invalid_cmd:      0
dsp_coproc_err: 0   comp_unsupported:0  pak_too_big:      0
null_packets:  0
pak_mp_length_spec_fault: 0
tx_lo_queue_size_max 0 cmd_unimplemented: 0
219 seconds since last clear of counters
Interrupts: 4      Immed: 3      HiPri ints: 0
LoPri ints: 0     POST Errs: 0  Alerts: 1
Unk Cmds: 0      UnexpCmds: 0
cgx_cmd_pending:0  packet_loop_max: 0  packet_loop_limit: 0

```

Table 25 describes significant fields shown in the display.

Table 25 *show crypto engine accelerator statistic Compression Statistics Descriptions*

Counter	Description
packets decompressed	Number of packets that were decompressed by the interface.
packets compressed	Number of packets that were compressed by the interface.
compressed bytes in	Number of compressed bytes that were presented to the compression algorithm from the input interface on decrypt.
encompassed bytes in	Number of uncompressed bytes (payload) that were presented to the compression algorithm from Cisco IOS on encrypt.
packets bypass compression	Number of packets that were not compressed because they were too small (<128 bytes).
packet abort compression	Number of packets that were not compressed because the packets are expanded rather than compressed.
packets fail compression	Number of packets that were not compressed because of problems in the compression algorithm.
compression ratio	Ratio of compression and decompression of packets presented to the compression algorithm that were successfully compressed or decompressed. This statistic measures the efficiency of the algorithm for all packets that were compressed or decompressed.
overall compression ratio	Ratio of compression and decompression of packets presented to the compression algorithm, including those that were not compressed due to expansion, too small. This ratio indicates whether the data traffic on this interface is suitable for compression. A ratio of 1:1 would imply that no successful compression is being performed on this data traffic.
decompressed bytes out	Number of decompressed bytes that were sent to Cisco IOS by the compression algorithm on decrypt.
compressed bytes out	Number of compressed bytes that were forwarded to Cisco IOS by the algorithm on encrypt.

The following sample output displays a typical output of the current statistics and error counters for the hardware accelerator of the router:

```

Router# show crypto engine accelerator statistic

Virtual Private Network (VPN) Module in slot :0

```

```

Statistics for Hardware VPN Module since the last clear
of counters 1379 seconds ago
  167874 packets in                167874 packets out
201596210 bytes in                201596059 bytes out
   121 paks/sec in                 121 paks/sec out
  1169 Kbits/sec in                1169 Kbits/sec out
    0 packets decrypted            0 packets encrypted
    0 bytes before decrypt         0 bytes encrypted
    0 bytes decrypted              0 bytes after encrypt
    0 packets decompressed         0 packets compressed
    0 bytes before decomp          0 bytes before comp
    0 bytes after decomp           0 bytes after comp
    0 packets bypass decompr       0 packets bypass compress
    0 bytes bypass decompress      0 bytes bypass compressi
    0 packets not decompress       0 packets not compressed
    0 bytes not decompressed       0 bytes not compressed
  1.0:1 compression ratio         1.0:1 overall
    20 commands out                20 commands acknowledged

Last 5 minutes:
  46121 packets in                46121 packets out
   153 paks/sec in                 153 paks/sec out
1667834 Kbits/sec in              1667836 Kbits/sec out
    0 bytes decrypted              0 bytes encrypted
    0 Kbits/sec decrypted          0 Kbits/sec encrypted
  1.0:1 compression ratio         1.0:1 overall

Errors:
ppq full errors      :      0 ppq rx errors      :      0
cmdq full errors    :      0 cmdq rx errors    :      0
no buffer           :      0 replay errors     :      0
dest overflow       :      0 authentication errors :      0
Out of memory       :      0 Access denied     :      0
Out of handles      :      0 Bad function code  :      0
Invalid parameter   :      0 Bad handle value  :      0
Output buffer overrun :      0 Input Underrun   :      0
Input Overrun       :      0 Invalid Key      :      0
Invalid Packet      :      0 Decrypt Failure  :      0
Verification Fail   :      0 Bad Attribute    :      0
Invalid attribute val:      0 Missing attribute :      0
Unwrappable object  :      0 Hash Miscompare  :      0
DF Bit set          :      0 RNG self test fail :      0
Other error         :      0
sessions            :      0

Warnings:
sessions_expired:0      packets_fragmented:0
general:                0

```

**Tips**

In Cisco IOS Release 12.2(8)T and later releases, you can add a time stamp to show commands using the **exec prompt timestamp** command in line configuration mode.

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.

Command	Description
crypto dynamic-map	Creates a dynamic map crypto configuration for a session.
crypto engine accelerator	Enables the use of the onboard hardware accelerator of the Cisco uBR905 and Cisco uBR925 routers for IPsec encryption.
crypto ipsec	Defines the IPsec SAs 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 transmit rings for the crypto engine.
show crypto engine accelerator sa-database	Displays the active (in-use) entries in the crypto engine security association (SA) database.
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.

show crypto ipsec client ezvpn

To display the Cisco Easy VPN Remote configuration, use the **show crypto ipsec client ezvpn** command in privileged EXEC mode.

show crypto ipsec client ezvpn

Syntax Description This command has no arguments or keywords.

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(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Examples The following example shows a typical display from the **show crypto ipsec client ezvpn** command for an active Virtual Private Network (VPN) connection when the router is in client mode:

```
Router# show crypto ipsec client ezvpn

Tunnel name: hw1
Inside interface list: FastEthernet0/0, Serial11/0,
Outside interface: Serial0/0
Current State: IPSEC_ACTIVE
Last Event: SOCKET_UP
Address: 209.165.201.0
Mask: 255.255.255.224
DNS Primary: 209.165.201.1
DNS Secondary: 209.165.201.2
NBMS/WINS Primary: 209.165.201.3
NBMS/WINS Secondary: 209.165.201.4
Default Domain: cisco.com
```

The following example shows a typical display from the **show crypto ipsec client ezvpn** command for an active VPN connection when the router is in network-extension mode:

```
Router# show crypto ipsec client ezvpn

Tunnel name: hw1
Inside interface list: FastEthernet0/0, Serial11/0,
Outside interface: Serial0/0
Current State: IPSEC_ACTIVE
Last Event: SOCKET_UP
Address: 209.165.202.128
Mask: 255.255.255.224
Default Domain: cisco.com
```

show crypto ipsec client ezvpn

```
Split Tunnel List: 1
  Address      : 209.165.200.225
  Mask        : 255.255.255.224
  Protocol    : 0x0
  Source Port : 0
  Dest Port   : 0
```

The following example shows a typical display from the **show crypto ipsec client ezvpn** command for an inactive VPN connection:

```
Router# show crypto ipsec client ezvpn
```

```
Current State: IDLE
Last Event: REMOVE INTERFACE CFG
Router#
```

[Table 26](#) describes significant fields shown by the **show crypto ipsec client ezvpn** command:

Table 26 *show crypto ipsec client ezvpn Field Descriptions*

Field	Description
Current State	Displays whether the VPN tunnel connection is active or idle. Typically, when the tunnel is up, the current state is IPSEC ACTIVE.
Last Event	Displays the last event performed on the VPN tunnel. Typically, the last event before a tunnel is created is SOCKET UP.
Address	Displays the IP address used on the outside interface.
Mask	Displays the subnet mask used for the outside interface.
DNS Primary	Displays the primary domain name system (DNS) server provided by the Dynamic Host Configuration Protocol (DHCP) server.
DNS Secondary	Displays the secondary DNS server provided by the DHCP server.
Domain Name	Displays the domain name provided by the DHCP server.
NBMS/WINS Primary	Displays the primary NetBIOS Microsoft Windows Name Server provided by the DHCP server.
NBMS/WINS Secondary	Displays the secondary NetBIOS Microsoft Windows Name Server provided by the DHCP server.

Related Commands

Command	Description
show crypto ipsec transform	Displays the specific configuration for one or all transformation sets.

show crypto ipsec sa

To display the settings used by current security associations (SAs), use the **show crypto ipsec sa** command in EXEC mode.

```
show crypto ipsec sa [map map-name | address | identity | interface interface | peer [vrf
  fvrf-name] address | vrf ivrf-name] [detail]
```

Syntax Description

map <i>map-name</i>	(Optional) Any existing SAs that were created for the crypto map set named <i>map-name</i> are displayed.
address	(Optional) All existing SAs are displayed, sorted by the destination address (either the local address or the address of the IP Security (IPSec) remote peer) and then by protocol (Authentication Header [AH] or Encapsulation Security Protocol [ESP]).
identity	(Optional) Only the flow information is displayed. It does not show the SA information.
interface <i>interface</i>	(Optional) All existing SAs created for an interface that is named <i>interface</i> are displayed.
peer [vrf <i>fvrf-name</i>] address	(Optional) All existing SAs with the peer address. If the peer address is in the Virtual Routing and Forwarding (VRF), specify vrf and the <i>fvrf-name</i> .
vrf <i>ivrf-name</i>	(Optional) All existing SAs whose inside virtual routing and forwarding (IVRF) is the same as the <i>ivrf-name</i> .
detail	(Optional) Detailed error counters are displayed. (The default is the high-level send or receive error counters.)

Command Modes

EXEC

Command History

Release	Modification
11.3 T	This command was introduced.
12.2(13)T	The “remote crypto endpt” and “in use settings” fields were modified to support Network Address Translation (NAT) traversal.
12.2(15)T	The interface keyword and <i>interface</i> argument were added. The peer keyword, the vrf keyword, and the <i>fvrf-name</i> argument were added. In addition, the address keyword was added to the peer keyword string. The vrf keyword and <i>ivrf-name</i> argument were added.

Usage Guidelines

If no keyword is used, all SAs are displayed. They are sorted first by interface, and then by traffic flow (for example, source or destination address, mask, protocol, or port). Within a flow, the SAs are listed by protocol (ESP or AH) and direction (inbound or outbound).

Examples

The following is sample output for the **show crypto ipsec sa** command:

```
Router# show crypto ipsec sa vrf vpn2

interface: Ethernet1/2
  Crypto map tag: ra, local addr. 172.16.1.1

protected vrf: vpn2
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (10.4.1.4/255.255.255.255/0/0)
current_peer: 10.1.1.1:500
  PERMIT, flags={}
  #pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0
  #pkts decaps: 0, #pkts decrypt: 0, #pkts verify 0
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0
  #pkts not decompressed: 0, #pkts decompress failed: 0
  #send errors 0, #recv errors 0

local crypto endpt.: 172.16.1.1, remote crypto endpt.: 10.1.1.1
path mtu 1500, media mtu 1500
current outbound spi: 50110CF8

inbound esp sas:
  spi: 0xA3E24AFD(2749516541)
    transform: esp-3des esp-md5-hmac ,
    in use settings ={Tunnel, }
    slot: 0, conn id: 5127, flow_id: 7, crypto map: ra
    sa timing: remaining key lifetime (k/sec): (4603517/3503)
    IV size: 8 bytes
    replay detection support: Y

inbound ah sas:

inbound pcp sas:

outbound esp sas:
  spi: 0x50110CF8(1343294712)
    transform: esp-3des esp-md5-hmac ,
    in use settings ={Tunnel, }
    slot: 0, conn id: 5128, flow_id: 8, crypto map: ra
    sa timing: remaining key lifetime (k/sec): (4603517/3502)
    IV size: 8 bytes
    replay detection support: Y

outbound ah sas:

outbound pcp sas:
```

The following configuration was in effect when the above **show crypto ipsec sa vrf** command was issued. The IPSec remote access tunnel was “UP” when this command was issued.

```
crypto dynamic-map vpn1 1
  set transform-set vpn1
  set isakmp-profile vpn1-ra
  reverse-route
!
crypto dynamic-map vpn2 1
  set transform-set vpn2
  set isakmp-profile vpn2-ra
  reverse-route
!
!
crypto map ra 1 ipsec-isakmp dynamic vpn1
```

```
crypto map ra 2 ipsec-isakmp dynamic vpn2
```

show crypto ipsec security-association lifetime

To display the security association (SA) lifetime value configured for a particular crypto map entry, use the **show crypto ipsec security-association lifetime** command in EXEC mode.

show crypto ipsec security-association lifetime

Syntax Description This command has no arguments or keywords.

Command Modes EXEC

Command History	Release	Modification
	11.3 T	This command was introduced.

Examples The following is sample output for the **show crypto ipsec security-association lifetime** command:

```
Router# show crypto ipsec security-association lifetime
Security-association lifetime: 4608000 kilobytes/120 seconds
```

The following configuration was in effect when the previous **show crypto ipsec security-association lifetime** command was issued:

```
crypto ipsec security-association lifetime seconds 120
```

show crypto ipsec transform-set

To display the configured transform sets, use the **show crypto ipsec transform-set** command in EXEC mode.

show crypto ipsec transform-set [*tag transform-set-name*]

Syntax Description

tag transform-set-name (Optional) Only the transform sets with the specified *transform-set-name* are displayed.

Command Modes

EXEC

Command History

Release	Modification
11.3 T	This command was introduced.
12.2(13)T	The command output was expanded to include a warning message for users who try to configure an IP Security (IPSec) transform that the hardware does not support.

Examples

The following is sample output for the **show crypto ipsec transform-set** command:

```
Router# show crypto ipsec transform-set

Transform set combined-des-sha: {esp-des esp-sha-hmac}
  will negotiate = { Tunnel, },

Transform set combined-des-md5: {esp-des esp-md5-hmac}
  will negotiate = { Tunnel, },

Transform set t1: {esp-des esp-md5-hmac}
  will negotiate = {Tunnel,,},

Transform set t100: {ah-sha-hmac}
  will negotiate = {Transport,,},

Transform set t2: {ah-sha-hmac}
  will negotiate = {Tunnel,,},
  { esp-des }
  will negotiate = {Tunnel,,},
```

The following configuration was in effect when the previous **show crypto ipsec transform-set** command was issued:

```
crypto ipsec transform-set combined-des-sha esp-des esp-sha-hmac
crypto ipsec transform-set combined-des-md5 esp-des esp-md5-hmac
crypto ipsec transform-set t1 esp-des esp-md5-hmac
crypto ipsec transform-set t100 ah-sha-hmac
  mode transport
crypto ipsec transform-set t2 ah-sha-hmac esp-des
```

The following sample output from the **show crypto ipsec transform-set** command displays a warning message after a user tries to configure an IPSec transform that the hardware does not support:

```
Router# show crypto ipsec transform-set

Transform set transform-1:{ esp-256-aes esp-md5-hmac  }
    will negotiate = { Tunnel,  },

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

show crypto isakmp key

To list the keyrings and their preshared keys, use the **show crypto isakmp key** command in EXEC mode.

show crypto isakmp key

Syntax Description This command has no arguments or keywords.

Command Modes EXEC

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

Examples The following is sample output for the **show crypto isakmp key** command:

```
Router# show crypto isakmp key

Hostname/Address      Preshared Key
vpn1                  : 172.61.1.1      vpn1
vpn2                  : 10.1.1.1        vpn2
```

The following configuration was in effect when the above **show crypto isakmp key** command was issued:

```
crypto keyring vpn1
  pre-shared-key address 172.16.1.1 key vpn1
crypto keyring vpn2
  pre-shared-key address 10.1.1.1 key vpn2
```

[Table 27](#) describes significant fields in the **show crypto isakmp key** profile.

Table 27 *show crypto isakmp key Field Descriptions*

Field	Description
Hostname/Address	The preshared key host name or address.
Preshared Key	The preshared key.
keyring	Name of the crypto keyring. The global keys are listed in the default keyring.
VRF string	The virtual route forwarding (VRF) of the keyring. If the keyring does not have a VRF, an empty string is printed.

show crypto isakmp policy

To display the parameters for each Internet Key Exchange (IKE) policy, use the **show crypto isakmp policy** command in EXEC mode.

show crypto isakmp policy

Syntax Description This command has no arguments or keywords.

Command Modes EXEC

Command History	Release	Modification
	11.3 T	This command was introduced.
	12.2(13)T	The command output was expanded to include a warning message for users who try to configure an IKE encryption method that the hardware does not support.

Examples

The following is sample output from the **show crypto isakmp policy** command, after two IKE policies have been configured (with priorities 15 and 20, respectively):

```
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
```



Note

Although the output shows “no volume limit” for the lifetimes, you can currently configure only a time lifetime (such as 86,400 seconds); volume limit lifetimes are not used.

The following sample output from the **show crypto isakmp policy** command displays a warning message after a user tries to configure an IKE encryption method that the hardware does not support:

```
Router# show crypto isakmp policy

Protection suite of priority 1
  encryption algorithm: AES - Advanced Encryption Standard (256 bit keys).
WARNING:encryption hardware does not support the configured
encryption method for ISAKMP policy 1
  hash algorithm:          Secure Hash Standard
  authentication method:  Pre-Shared Key
  Diffie-Hellman group:   #1 (768 bit)
  lifetime:               3600 seconds, no volume limit
```

Related Commands

Command	Description
authentication (IKE policy)	Specifies the authentication method within an IKE policy.
crypto isakmp policy	Defines an IKE policy.
encryption (IKE policy)	Specifies the encryption algorithm within an IKE policy.
group (IKE policy)	Specifies the DH 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 profile

To list all the Internet Security Association and Key Management Protocol (ISAKMP) profiles that are defined on a router, use the **show crypto isakmp profile** command in EXEC mode.

show crypto isakmp profile

Syntax Description This command has no arguments or keywords.

Command Modes EXEC

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

Examples The following is sample output for the **show crypto isakmp profile** command:

```
Router# show crypto isakmp profile

ISAKMP PROFILE vpn1-ra
  Identities matched are:
group vpn1-ra
  Identity presented is: ip-address
```

[Table 28](#) describes significant fields in the display.

Table 28 *show crypto isakmp profile Field Descriptions*

Field	Description
ISAKMP PROFILE	Name of the ISAKMP profile.
Identities matched are:	Lists all identities that the ISAKMP profile will match.
Identity presented is:	The identity that the ISAKMP profile will present to the remote endpoint.

The following configuration was in effect when the above **show crypto isakmp profile** command was issued:

```
crypto isakmp profile vpn1-ra
vrf vpn1
self-identity address
match identity group vpn1-ra
client authentication list aaa-list
isakmp authorization list aaa
client configuration address initiate
client configuration address respond
```

Related Commands	Command	Description
	show crypto isakmp key	Lists the keyrings and their preshared keys.

show crypto isakmp sa

To display all current Internet Key Exchange (IKE) security associations (SAs) at a peer, use the **show crypto isakmp sa** command in EXEC mode.

show crypto isakmp sa

Syntax Description This command has no arguments or keywords.

Command Modes EXEC

Command History	Release	Modification
	11.3 T	This command was introduced.

Examples The following is sample output from the **show crypto isakmp sa** command after IKE negotiations have been successfully completed between two peers:

```
Router# show crypto isakmp sa

f_vrf/i_vrf      dst          src          state        conn-id    slot
  /vpn2         172.21.114.123 10.1.1.1    QM_IDLE         13         0
```

[Table 29](#) through [Table 32](#) show the various states that may be displayed in the output of the **show crypto isakmp sa** command. When an Internet Security Association and Key Management Protocol (ISAKMP) SA exists, it will most likely be in its quiescent state (QM_IDLE). For long exchanges, some of the MM_xxx states may be observed.

Table 29 States in Main Mode Exchange

State	Explanation
MM_NO_STATE	The ISAKMP SA has been created, but nothing else has happened yet. It is “larval” at this stage—there is no state.
MM_SA_SETUP	The peers have agreed on parameters for the ISAKMP SA.
MM_KEY_EXCH	The peers have exchanged Diffie-Hellman public keys and have generated a shared secret. The ISAKMP SA remains unauthenticated.
MM_KEY_AUTH	The ISAKMP SA has been authenticated. If the router initiated this exchange, this state transitions immediately to QM_IDLE, and a Quick Mode exchange begins.

Table 30 States in Aggressive Mode Exchange

State	Explanation
AG_NO_STATE	The ISAKMP SA has been created, but nothing else has happened yet. It is “larval” at this stage—there is no state.
AG_INIT_EXCH	The peers have done the first exchange in aggressive mode, but the SA is not authenticated.
AG_AUTH	The ISAKMP SA has been authenticated. If the router initiated this exchange, this state transitions immediately to QM_IDLE, and a quick mode exchange begins.

Table 31 States in Quick Mode Exchange

State	Explanation
QM_IDLE	The ISAKMP SA is idle. It remains authenticated with its peer and may be used for subsequent quick mode exchanges. It is in a quiescent state.

Table 32 show crypto isakmp sa Field Descriptions

Field	Description
f_vrf/i_vrf	The front door virtual routing and forwarding (FVRF) and the inside VRF (IVRF) of the IKE SA. If the FVRF is global, the output shows f_vrf as an empty field.

Related Commands

Command	Description
crypto isakmp policy	Defines an IKE policy.
lifetime (IKE policy)	Specifies the lifetime of an IKE SA.