show crypto ace redundancy

To display information about a Blade Failure Group, use the **show crypto ace redundancy** command in privileged EXEC mode.

show crypto ace redundancy

Defaults

No default behavior or values.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(18)SXE2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example shows information about a Blade Failure Group that has a group ID of 1 and consists of two IPSec VPN SPAs—one IPSec VPN SPA is in slot 3, subslot 0 and one IPSec VPN SPA is in slot 5, subslot 0:

```
Router# show crypto ace redundancy
---------------------------------------
LC Redundancy Group ID            :1
Pending Configuration Transactions:0
Current State                     :OPERATIONAL
Number of blades in the group     :2
Slots
---------------------------------------
Slot:3 Subslot:0
Slot state:0x36
Booted
Received partner config
Completed Bulk Synchronization
Crypto Engine in Service
Rebooted 22 times
Initialization Timer not running
Slot:5 Subslot:0
Slot state:0x36
Booted
Received partner config
Completed Bulk Synchronization
Crypto Engine in Service
Rebooted 24 times
Initialization Timer not running

ACE B2B Group State:OPERATIONAL Event:BULK DONE
ACE B2B Group State:CREATED Event:CONFIG_DOWNLOAD_DONE
ACE B2B Group State:DELETED Event:CONFIG_DELETE
ACE B2B Group State:OPERATIONAL Event:BULK DONE
```

```
ACE B2B Group State:CREATED Event:CONFIG_DOWNLOAD_DONE
ACE B2B Group State:DELETED Event:CONFIG_DELETE
ACE B2B Group State:OPERATIONAL Event:CONFIG_DOWNLOAD_DONE
ACE B2B Group State:DELETED Event:CONFIG_ADD
ACE B2B Group State:CREATED Event:UNDEFINED B2B HA EVENT
ACE B2B Group State:CREATED Event:CONFIG_DOWNLOAD_DONE
```

Related Commands

Command	Description
linecard-group feature card	Assigns a group ID to a Blade Failure Group.
redundancy	Enters redundancy configuration mode.
show redundancy linecard-group	Displays the components of a Blade Failure Group.

show crypto ca certificates

Note This command was replaced by the **show crypto pki certificates** command effective with Cisco IOS Release 12.3(7)T.

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

show crypto ca certificates

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged 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 pki enroll** command)
- The certificate of the CA, if you have received the CA's certificate (see the **crypto pki authenticate** command)
- RA certificates, if you have received RA certificates (see the **crypto pki 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 pki 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 pki authenticate	Authenticates the CA (by obtaining the certificate of the CA).
crypto pki 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

Note This command was replaced by the **show crypto pki crls** command effective with Cisco IOS Release 12.3(7)T.

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

show crypto ca crls

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged 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 pki 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

Note This command was replaced by the **show crypto pki timers** command effective with Cisco IOS Release 12.3(8)T.

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 privileged EXEC mode.

show crypto ca timers

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.

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 pki trustpoint	Declares the CA that your router should use.

show crypto ca trustpoints

Note This command was replaced by the **show crypto pki trustpoints** command effective with Cisco IOS Release 12.3(7)T and 12.2(18)SXD.

To display the trustpoints that are configured in the router, use the **show crypto pki trustpoints** command in privileged EXEC or user EXEC mode.

show crypto ca trustpoints

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)
User EXEC (>)

Command History

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

Usage Guidelines

This command replaces 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 pki 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 pki trustpoint	Declares the CA that your router should use.

show crypto call admission statistics

To monitor Crypto Call Admission Control (CAC) statistics, use the **show crypto call admission statistics** command in user EXEC or privileged EXEC mode.

show crypto call admission statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.2(18)SXD1	This command was integrated into Cisco IOS Release 12.2(18)SXD1.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
15.1(3)T	This command was modified. The output of this command was updated to display information about IPsec SAs.

Usage Guidelines

Enter this command to display information about the Crypto CAC configuration parameters and their history, including statistics regarding the current security association (SA) count, SAs being negotiated, total new SA requests, the number of Internet Key Exchange (IKE) and IPsec SA requests accepted and rejected, and details regarding why requests were rejected.

Examples

The following is sample output from the **show crypto call admission statistics** command:

```
Router# show crypto call admission statistics

----------------------------------------------------------------------
               Crypto Call Admission Control Statistics
----------------------------------------------------------------------
System Resource Limit:      111 Max IKE SAs:     0 Max in nego:  1000
Total IKE SA Count:           0 active:          0 negotiating:     0
Incoming IKE Requests:        0 accepted:        0 rejected:        0
Outgoing IKE Requests:        0 accepted:        0 rejected:        0
Rejected IKE Requests:        0 rsrc low:        0 Active SA limit: 0
                                                   In-neg SA limit: 0
IKE packets dropped at dispatch:        0

Max IPSEC SAs:   111
Total IPSEC SA Count:           0 active:          0 negotiating:     0
Incoming IPSEC Requests:        0 accepted:        0 rejected:        0
Outgoing IPSEC Requests:        0 accepted:        0 rejected:        0

Phase1.5 SAs under negotiation:         0
```

Table 82 describes the significant fields shown in the display.

Table 82 show crypto call admission statistics Field Descriptions

Field	Description
System Resource Limit	Percentage of system resources that a router is using before IKE starts dropping all SA requests.
Max IKE SAs	Number of active IKE SA requests allowed on the router.
Total IKE SA Count	Number of IKE SAs.
active	Number of active SAs.
negotiating	Number of SA requests being negotiated.
Incoming IKE Requests	Number of incoming IKE SA requests.
Incoming IKE Requests accepted	Number of accepted IKE SA requests.
Incoming IKE Requests rejected	Number of rejected incoming IKE SA requests.
Outgoing IKE Requests	Number of outgoing IKE SA requests.
Outgoing IKE requests accepted	Number of accepted outgoing IKE SA requests.
Outgoing IKE requests rejected	Number of rejected outgoing IKE SA requests.
Rejected IKE Requests	Number of IKE requests that were rejected.
rsrc low	Number of IKE requests that were rejected because system resources were low or the preconfigured system resource limit was exceeded.
SA limit	Number of IKE SA requests that were rejected because the SA limit has been reached.
Incoming IPSEC Requests	Number of incoming IPsec SA requests.
Incoming IPSEC Requests accepted	Number of accepted IPsec SA requests.
Incoming IPSEC Requests rejected	Number of rejected incoming IPsec SA requests.
Outgoing IPSEC Requests	Number of outgoing IPsec SA requests.
Outgoing IPSEC requests accepted	Number of accepted outgoing IPsec SA requests.
Outgoing IPSEC requests rejected	Number of rejected outgoing IPsec SA requests.
Phase1.5 SAs	Number of negotiations in XAUTH or configuration exchange mode.

Related Commands

Command	Description
clear crypto call admission statistics	Clears the counters that track the number of accepted and rejected IKE SA requests.

show crypto ctcp

To display information about a Cisco Tunnel Control Protocol (cTCP) session, use the **show crypto ctcp** command in privileged EXEC mode.

show crypto ctcp [**peer** *ip-address*] [**detail**]

Syntax Description

peer	(Optional) Displays information about a specific peer.
ip-address	(Optional) IP address of the specific peer.
detail	(Optional) Displays information about the local TCP sequence number and the TCP sequence number of the packets for the peer.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(9)T	This command was introduced.

Examples

The following **show** command output displays detailed information about a specific peer:

```
Router# show crypto ctcp peer 10.76.235.21 detail

    Remote                  Local                VRF                  Status

    10.76.235.21:3519       10.76.248.239:10000                       CTCP_ACK_R
                            LocalSeq#6807392F    RemoteSeq#010116C7
```

Table 83 provides information about significant fields in the display.

Table 83 show crypto ctcp Field Descriptions

Field	Description
Remote	IP address of the remote peer with which this cTCP session is set up.
Local	IP address of the server to which the cTCP packets are addressed.
VRF	Name of the Virtual Private Network routing and forwarding (VRF) instance to which this session belongs. If the VRF is blank, the global routing table is used.
Status	Status of the cTCP session. CTCP_ACK_R is a successful cTCP setup. Any other state indicates that cTCP is not yet set up or failed to be set up.
LocalSeq	Sequence number of the last Transmission Control Protocol (TCP) packet sent by the server on this connection.
RemoteSeq	Sequence number of the last TCP packet that was received by the peer on this connection.

Related Commands

Command	Description
crypto ctcp	Configures cTCP encapsulation for Easy VPN.

show crypto datapath

To display the counters that help troubleshoot an encrypted data path, use the **show crypto datapath** command in privileged EXEC mode.

show crypto datapath {**ipv4** | **ipv6**} {**realtime** | **snapshot**} {**all** | **non-zero**} [**error** | **internal** | **punt** | **success**]

Syntax Description

ipv4	Designate IPv4 is used in the network.
ipv6	Designate IPv6 is used in the network.
realtime	Displays the counters that capture traffic statistics as they occur.
snapshot	Displays the counters that capture traffic statistics as of a single point in time.
all	Display all counters.
non-zero	Display all counters that have at least one event recorded.
error	(Optional) Display the packet processing and dropped packet errors.
internal	(Optional) Track the movement of a packet from end to end across an encrypted data path.
punt	(Optional) Display the instances when the configured processing method failed, and an alternative was used.
success	(Optional) Display the interfaces where packets were successfully processed.

Command Default

The command defaults are:

- IP version: **ipv4**
- Counters: **all**
- Display time: **realtime**

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

Use the **show crypto datapath counters** command to troubleshoot an encrypted data path.

Note Cisco recommends use of this command only for troubleshooting under the guidance of a Cisco TAC engineer.

You must specify the IP version used in the network. You can display all counters, only the counters that have recorded events, or one of these specific counters:

- Error counters track packet processing errors and associated packet drops. When a packet encounters an error, the first 64 bytes of that packet are stored in a buffer, to facilitate troubleshooting.
- Internal counters show the detailed movement of a packet, end to end, across an encrypted data path.
- Punt counters track instances when the configured packet processing method failed, and an alternative method was used. Because such instances might indicate a problem, it is useful to track them.
- Success counters help diagnose network performance problems. Frequently, although a network is configured for fast switching or CEF, packets are using a slower path. Success counters record the interfaces in the data path where packets were successfully processed and reveal the actual processing path.

You must also choose the display timeframe for the counters:

- The **realtime** option captures traffic statistics as they occur, and results in significant discrepancies between the first data reports and later data, because the counters increment with the traffic flow. This is the default option.
- The **snapshot** option captures traffic statistics as of a specific point in time, and results in a close match among all counts, because the counters do not increment with the continuing traffic flow.

Examples

The following example shows output from the **show crypto datapath** command. In this example, the **snapshot** option is specified for the timeframe, and only counters that have recorded events are displayed. The output of this command is intended for use by Cisco TAC engineers.

```
Router# show crypto datapath ipv4 snapshot non-zero

Success Statistics: Snapshot at 21:34:30 PST Mar 4 2006
  crypto check input core
    2nd round ok:            245      1st round ok:            118
  post crypto ip encrypt
    post encrypt ipflowok:   230
  crypto ceal post encrypt switch
    post encrypt ipflowok-2: 230
Error Statistics: Snapshot at 21:34:30 PST Mar 4 2006
Punt Statistics: Snapshot at 21:34:30 PST Mar 4 2006
  crypto ceal post decrypt switch
    fs to ps:                245
Internal Statistics: Snapshot at 21:34:30 PST Mar 4 2006
  crypto check input
    check input core not con 378      check input core consume 623

  crypto check input core
    came back from ce:       245      deny pak:                15

  crypto ipsec les fs
    not esp or ah:           1113
  post crypto ip decrypt
    decrypt switch:          245
  crypto decrypt ipsec sa check
    check ident success:     245
  crypto ceal post decrypt switch
    fs:                      245
  crypto ceal post decrypt fs
    les ip turbo fs:         245      tunnel ip les fs:        245
```

```
crypto ceal post decrypt ps
  proc inline:             245
crypto ceal punt to process inline
  coalesce:                245      simple enq:              245

crypto ceal post encrypt switch
  ps:                      230
crypto ceal post encrypt ps
  ps coalesce:             230      simple enq:              230

crypto engine ps vec
  ip encrypt:              230
crypto send epa packets
  ucast next hop:          230      ip ps send:              230
```

Related Commands

Command	Description
show monitor event-trace	Displays contents of error history buffers.

show crypto debug-condition

To display crypto debug conditions that have already been enabled in the router, use the **show crypto debug-condition** command in privileged EXEC mode.

show crypto debug-condition {[**peer**] [**connid**] [**spi**] [**fvrf**] [**gdoi-group** *groupname*] [**isakmp profile** *profile-name*] [**ivrf**] [**local** *ip-address*] [**unmatched**] [**username** *username*]}

Syntax Description

peer	(Optional) Displays debug conditions related to the peer. Possible conditions can include peer IP address, subnet mask, hostname, username, and group key.
connid	(Optional) Displays debug conditions related to the connection ID.
spi	(Optional) Displays debug conditions related to the security parameter index (SPI).
fvrf	(Optional) Displays debug conditions related to the front-door virtual private network (VPN) routing and forwarding (FVRF) instance.
gdoi-group *groupname*	(Optional) Displays debug conditions related to the Group Domain of Interpretation (GDOI) group filter. • The *groupname* value is the name of the GDOI group.
isakmp profile *profile-name*	(Optional) Displays debug conditions related to the Internet Security Association Key Management Protocol (ISAKMP) profile filter. • The *profile-name* value is the name of the profile filter.
ivrf	(Optional) Displays debug conditions related to the inside VRF (IVRF) instance.
local *ip-address*	(Optional) Displays debug conditions related to the local address debug condition filters. • The *ip-address* is the IP address of the local crypto endpoint.
unmatched	(Optional) Displays debug messages related to the Internet Key Exchange (IKE), IP Security (IPsec), or the crypto engine, depending on what was specified via the **debug crypto condition unmatched** [**engine** | **gdoi-group** | **ipsec** | **isakmp**] command.
username *username*	(Optional) Displays debug messages related to the AAA Authentication (Xauth) or public key infrastructure (PKI) and authentication, authorization, and accounting (AAA) username filter.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Release	Modification
12.4(11)T	The **gdoi-group** *groupname*, **isakmp profile** *profile-name*, **local** *ip-address*, and **username** *username* keywords and arguments were added.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

You can specify as many filter values as specified via the **debug crypto condition** command. (You cannot specify a filter value that you did not use in the **debug crypto condition** command.)

Examples

The following example shows how to display debug messages when the peer IP address is 10.1.1.1, 10.1.1.2, or 10.1.1.3 and when the connection ID 2000 of crypto engine 0 is used. This example also shows how to enable global debug crypto CLIs and enable the **show crypto debug-condition** command to verify conditional settings.

```
Router# debug crypto condition connid 2000 engine-id 1
Router# debug crypto condition peer ipv4 10.1.1.1
Router# debug crypto condition peer ipv4 10.1.1.2
Router# debug crypto condition peer ipv4 10.1.1.3
Router# debug crypto condition unmatched
! Verify crypto conditional settings.
Router# show crypto debug-condition

Crypto conditional debug currently is turned ON
IKE debug context unmatched flag:ON
IPsec debug context unmatched flag:ON
Crypto Engine debug context unmatched flag:ON

IKE peer IP address filters:
10.1.1.1  10.1.1.2   10.1.1.3

Connection-id filters:[connid:engine_id]2000:1,
! Enable global crypto CLIs to start conditional debugging.
Router# debug crypto isakmp
Router# debug crypto ipsec
Router# debug crypto engine
```

The following example shows how to disable all crypto conditional settings via the **reset** keyword:

```
Router# debug crypto condition reset
! Verify that all crypto conditional settings have been disabled.
Router# show crypto debug-condition

Crypto conditional debug currently is turned OFF
IKE debug context unmatched flag:OFF
IPsec debug context unmatched flag:OFF
Crypto Engine debug context unmatched flag:OFF
```

Related Commands

Command	Description
debug crypto condition	Defines conditional debug filters.
debug crypto condition unmatched	Displays crypto conditional debug messages when context information is unavailable to check against debug conditions.

show crypto dynamic-map

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

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.3 T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

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 eli

To display how many IKE-SAs and IPSec sessions are active and how many Diffie-Hellman keys are in use for each hardware crypto engine, use the **show crypto eli** in user EXEC or privileged EXEC mode.

show crypto eli

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.1(5)E	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS release 12.2(33)SXH.

Usage Guidelines

Use this command to obtain a snapshot of how many Internet Key Exchange (IKE) and IP Security (IPSec) sessions are active and how many Diffie-Hellman keys are in use for each hardware crypto engine. The **show crypto eli** command also allows you to see how far an ISA is from reaching its maximum limit.

Note IKE is a key management protocol standard that is used in conjunction with the IPSec standard. IPSec can be configured without IKE. However, IKE enhances IPSec by providing additional features, flexibility, and ease of configuration for the IPSec standard. When IKE is used with IPSec, IKE automatically negotiates the IPSec security associations (SAs).

(The eli component of the command calls the Encryption Layer Interface.)

Examples

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

```
Router# show crypto eli

Encryption Layer :  ACTIVE
 Number of crypto engines = 2.

 Slot-3 crypto engine details.
 Capability-IPSec :No-IPPCP, 3DES, NoRSA

 IKE-Session   :    0 active,  2029 max, 0 failed
 DH-Key        :    0 active,  1014 max, 0 failed
 IPSec-Session :    0 active,  4059 max, 0 failed
```

```
 Slot-5 crypto engine details.
 Capability-IPSec :No-IPPCP, 3DES, NoRSA

 IKE-Session   :    0 active,  2029 max, 0 failed
 DH-Key        :    0 active,  1014 max, 0 failed
 IPSec-Session :    0 active,  4059 max, 0 failed
```

The following is sample output for the **show crypto eli** command for the IPSec VPN SPA:

```
Router# show crypto eli

>>Hardware Encryption : ACTIVE
>> Number of hardware crypto engines = 2
>>
>> CryptoEngine SPA-IPSEC-2G[3/0] details: state = Active
>> Capability      :
>>     IPSEC: DES, 3DES, AES, RSA
>>
>> IKE-Session   :     0 active, 16383 max, 0 failed
>> DH            :     0 active,  9999 max, 0 failed
>> IPSec-Session :     0 active, 65534 max, 0 failed
>>
>> CryptoEngine SPA-IPSEC-2G[3/1] details: state = Active
>> Capability      :
>>     IPSEC: DES, 3DES, AES, RSA
>>
>> IKE-Session   :     1 active, 16383 max, 0 failed
>> DH            :     0 active,  9999 max, 0 failed
>> IPSec-Session :     2 active, 65534 max, 0 failed
```

Table 84 describes significant fields shown in the display.

Table 84 show crypto eli summary Field Descriptions

Field	Description
active	The number of sessions that are active on a given hardware crypto engine.
max	The maximum number of sessions allowed for any given IKE, DH, or IPSec entry.
failed	The number of times that Cisco IOS software attempted to create more sessions than the number specified in “max.”

show crypto eng qos

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

show crypto eng qos

Syntax Description

This command has no keywords or arguments.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(13)T	This command was introduced in Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **show crypto eng qos** command to determine if QoS is enabled on LLQ for IPSec encryption engines.

Examples

The following example shows how to determine if 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

To display a summary of the configuration information for the crypto engines, use the **show crypto engine** command in privileged EXEC mode.

show crypto engine {**accelerator** {**statistic** | **ring** {**control** | **packet** | **pool**}} | **brief** | **configuration** | **connections** {**active** | **dh** | **dropped-packet** | **flow**} | **qos** | **token** [**detail**]}

Syntax Description

accelerator	Displays crypto accelerator information.
statistic	Displays crypto accelerator statistic information.
ring	Displays crypto accelerator ring information.
control	Displays control ring information.
packet	Displays packet ring information.
pool	Displays pool ring information.
brief	Displays a summary of the configuration information for the crypto engine.
configuration	Displays the version and configuration information for the crypto engine.
connections	Displays information about the crypto engine connections.
active	Displays all active crypto engine connections.
dh	Displays crypto engine Diffie-Hellman table entries.
dropped-packet	Displays crypto engine dropped packets.
flow	Displays crypto engine flow table entries.
qos	Displays quality of service (QoS) information. • This keyword has a null output if any advanced integration module (AIM) except AIM-VPN/SSL-1 is used. The command-line interface (CLI) will accept the command, but there will be no output.
token	Displays the crypto token engine information.
detail	(Optional) Displays the detailed information of the crypto token engine.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.2	This command was introduced on the Cisco 7200, RSP7000, and 7500 series routers.
12.2(15)ZJ	This command was implemented for the AIM-VPN/BPII on the following platforms: Cisco 2610XM, Cisco 2611XM, Cisco 2620XM, Cisco 2621XM, Cisco 2650XM, and Cisco 2651XM.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.4(4)T	IPv6 address information was added to command output.
12.4(9)T	AIM-VPN/SSL-3 encryption module information was added to command output.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Release	Modification
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(22)T	The **token** and **detail** keywords were added.
Cisco IOS XE Release 2.2	This command was integrated into Cisco IOS XE Release 2.2. The **accelerator**, **control, packet, pool, ring**, and **static** keywords were added.

Usage Guidelines

This command displays all crypto engines and displays the AIM-VPN product name.

If a hardware crypto engine does not support native Group Domain of Interpretation (GDOI) header preservation, the **show crypto engine connections active** output for Group Encrypted Transport VPN (GET VPN) IP security (IPsec) connections displays a disallowed IP address of 0.0.0.0 (see the **show crypto engine connections active** "Examples" section).

Examples

The following is sample output from the **show crypto engine brief** command shows typical crypto engine summary information:

```
Router# show crypto engine brief

crypto engine name:  Virtual Private Network (VPN) Module
        crypto engine type:  hardware
                     State:  Enabled
                  Location:  aim 0
    VPN Module in slot:  0
          Product Name:  AIM-VPN/SSL-3
     Software Serial #:  55AA
             Device ID:  001F - revision 0000
             Vendor ID:  0000
          Revision No:  0x001F0000
          VSK revision:  0
          Boot version:  255
           DPU version:  0
           HSP version:  3.3(18) (PRODUCTION)
          Time running:  23:39:30
               Compression:  Yes
                       DES:  Yes
                   3 DES:  Yes
                 AES CBC:  Yes (128,192,256)
                AES CNTR:  No
     Maximum buffer length:  4096
          Maximum DH index:  3500
          Maximum SA index:  3500
        Maximum Flow index:  7000
      Maximum RSA key size:  2048


        crypto engine name:  Cisco VPN Software Implementation
        crypto engine type:  software
             serial number:  CAD4FCE1
      crypto engine state:  installed
     crypto engine in slot:  N/A
```

Table 85 describes the significant fields shown in the display.

Table 85 show crypto engine brief Field Descriptions

Field	Description
crypto engine name	Name of the crypto engine as assigned with the *key-name* argument in the **crypto key generate dss** command.
crypto engine type	If "software" is listed, the crypto engine resides in either the Route Switch Processor (RSP) (the Cisco IOS crypto engine) or in a second-generation Versatile Interface Processor (VIP2). If "crypto card" or "Encryption Service Adapter" (ESA) is listed, the crypto engine is associated with an ESA.
crypto engine state	The state "installed" indicates that a crypto engine is located in the given slot, but it is not configured for encryption. The state "dss key generated" indicates the crypto engine found in that slot has Digital Signature Standard (DSS) keys already generated.
crypto engine in slot	Chassis slot number of the crypto engine. For the Cisco IOS crypto engine, this is the chassis slot number of the RSP.

The following is sample output from **show crypto engine** command shows IPv6 information:

```
Router# show crypto engine connections

    ID Interface  Type  Algorithm           Encrypt  Decrypt IP-Address
     1 Et2/0      IPsec MD5                       0       46 FE80::A8BB:CCFF:FE01:2C02
     2 Et2/0      IPsec MD5                      41        0 FE80::A8BB:CCFF:FE01:2C02
     5 Tu0        IPsec SHA+DES                   0        0
3FFE:2002::A8BB:CCFF:FE01:2C02
     6 Tu0        IPsec SHA+DES                   0        0
3FFE:2002::A8BB:CCFF:FE01:2C02
  1001 Tu0        IKE   SHA+DES                   0        0
3FFE:2002::A8BB:CCFF:FE01:2C02
```

The following **show crypto engine** command output displays information for a situation in which a hardware crypto engine does not support native GDOI:

```
Router# show crypto engine connections active

Crypto Engine Connections

ID Interface     Type  Algorithm           Encrypt  Decrypt IP-Address
1079 Se0/0/0.10  IPsec AES+SHA                  0        0 0.0.0.0
1080 Se0/0/0.10  IPsec AES+SHA                  0        0 0.0.0.0
4364 <none>      IKE   SHA+3DES                 0        0
4381 <none>      IKE   SHA+3DES                 0        0
```

Related Commands

Command	Description
crypto engine accelerator	Enables the use of the onboard hardware accelerator for IPSec encryption.

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 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 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.
12.2(15)ZJ	This command was implemented for the AIM-VPN/BPII on the following platforms: Cisco 2610XM, Cisco 2611XM, Cisco 2620XM, Cisco 2621XM, Cisco 2650XM, and Cisco 2651XM.
12.3(4)T	The AIM-VPN/BPII was integrated into Cisco IOS Release 12.3(4)T on the following platforms: Cisco 2610XM, Cisco 2611XM, Cisco 2620XM, Cisco 2621XM, Cisco 2650XM, and Cisco 2651XM.

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 IP Security (IPsec) encryption statistics and error counters for the onboard hardware accelerator of the router or the IPsec Virtual Private Network (VPN) Shared Port Adapter (SPA), use the **show crypto engine accelerator statistic** command in privileged EXEC mode.

show crypto engine accelerator statistic

IPsec VPN SPA (SPA-IPSEC-2G) and VSPA (WS-IPSEC-3G)

show crypto engine accelerator statistic [**slot** *slot/subslot* | **all**] [**coreutil** | **detail**]

Syntax Description

slot *slot/subslot*	(IPsec VPN SPA and VSPA only—Optional) Chassis slot number and secondary slot number on the SPA Interface Processor (SIP) where the SPA is installed. Refer to the appropriate hardware manual for slot information. For SIPs, refer to the platform-specific SPA hardware installation guide or the corresponding "Identifying Slots and Subslots for SIPs and SPAs" topic in the platform-specific SPA software configuration guide. Displays platform statistics for the corresponding SPA. This output will not include network interface controller statistics.
all	(IPsec VPN SPA and VSPA only—Optional) Displays platform statistics for all IPsec VPN SPAs or VSPAs on the router. This output will not include network interface controller statistics.
coreutil	(VSPA only—Optional) Displays VPN core utilization statistics.
detail	(IPsec VPN SPA and VSPA only—Optional) Displays platform statistics for the SPA and network interface controller statistics. Note that the controller statistics contain Layer 2 (L2) counters.

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 output for this **show** command was enhanced to display compression statistics.
12.2(15)ZJ	This command was implemented for the AIM-VPN/BPII on the following platforms: Cisco 2610XM, Cisco 2611XM, Cisco 2620XM, Cisco 2621XM, Cisco 2650XM, and Cisco 2651XM.

Release	Modification
12.3(4)T	The AIM-VPN/BPII was integrated into Cisco IOS Release 12.3(4)T on the following platforms: Cisco 2610XM, Cisco 2611XM, Cisco 2620XM, Cisco 2621XM, Cisco 2650XM, and Cisco 2651XM.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA to support the IPsec VPN SPA on Cisco 7600 series routers.
12.4(9)T	Output was added for the AIM-VPN Secure Sockets Layer (SSL) encryption module.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH to support the IPsec VPN SPA on Catalyst 6500 series switches.
12.2(33)SXI	The **coreutil** keyword was added for the VSPA, and output was added to display the percent utilization with other utilization statistics in the crypto engine.
12.4(24)T	Output was modified to display reassembly and fragmentation-drop counters for VPN Service Adaptor (VSA) traffic statistics.

Usage Guidelines

No specific usage guidelines apply to the hardware accelerators.

IPsec VPN SPA and VSPA

Enter the **slot** keyword to display platform statistics for the corresponding SPA. This output will not include network interface controller statistics.

Enter the **all** keyword to display platform statistics for all IPsec VPN SPAs and VSPAs on the router. This output will not include network interface controller statistics.

Enter the **detail** keyword to display platform statistics for the SPA and network interface controller statistics. Note that the controller statistics contain L2 counters.

VSPA

Enter the **coreutil** keyword to display VPN core utilization statistics. This output will not include network interface controller statistics.

Tip 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.

Examples

Hardware VPN Module

The following example displays compression statistics for a hardware VPN module:

```
Router# show crypto engine accelerator statistic

Device:   AIM-VPN/SSL-3
Location: AIM Slot: 0
Virtual Private Network (VPN) Module in slot : 0
    Statistics for Hardware VPN Module since the last clear
     of counters 85319 seconds ago
               560 packets in                        560 packets out
             95600 bytes in                       124720 bytes out
                 0 paks/sec in                         0 paks/sec out
                 0 Kbits/sec in                        0 Kbits/sec out
```

```
                0 packets decrypted                   560 packets encrypted
                0 bytes before decrypt             124720 bytes encrypted
                0 bytes decrypted                   95600 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 compres
                0 bytes bypass decompres                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
            10426 commands out                      10426 commands acknowledged
    Last 5 minutes:
                0 packets in                            0 packets out
                0 paks/sec in                           0 paks/sec out
                0 bits/sec in                           0 bits/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
   ppq down errors          :        0   cmdq down errors         :        0
   no buffer                :        0   replay errors            :        0
   dest overflow            :        0   authentication errors    :        0
   Other error              :        0   Raw Input Underrun       :        0
   IPSEC Unsupported Option:        0   IPV4 Header Length       :        0
   ESP Pad Length           :        0   IPSEC Decompression      :        0
   AH ESP seq mismatch      :        0   AH Header Length         :        0
   AH ICV Incorrect         :        0   IPCOMP CPI Mismatch      :        0
   IPSEC ESP Modulo         :        0   Unexpected IPV6 Extensio:        0
   Unexpected Protocol      :        0   Dest Buf overflow        :        0
   IPSEC Pkt is fragment    :        0   IPSEC Pkt src count      :        0
   Invalid IP Version       :        0   Unwrappable              :        0
   SSL Output overrun       :        0   SSL Decompress failure   :        0
   SSL BAD Decomp History   :        0   SSL Version Mismatch     :        0
   SSL Input overrun        :        0   SSL Conn Modulo          :        0
   SSL Input Underrun       :        0   SSL Connection closed    :        0
   SSL Unrecognised content:        0   SSL record header length:        0
   PPTP Duplicate packet    :        0   PPTP Exceed max missed p:        0
   RNG self test fail       :        0   DF Bit set               :        0
   Hash Miscompare          :        0   Unwrappable object       :        0
   Missing attribute        :        0   Invalid attrribute value:        0
   Bad Attribute            :        0   Verification Fail        :        0
   Decrypt Failure          :        0   Invalid Packet           :        0
   Invalid Key              :        0   Input Overrun            :        0
   Input Underrun           :        0   Output buffer overrun    :        0
   Bad handle value         :        0   Invalid parameter        :        0
   Bad function code        :        0   Out of handles           :        0
   Access denied            :        0   Out of memory            :        0
   NR overflow              :        0   pkts dropped             :        0

Warnings:
   sessions_expired         :        0   packets_fragmented       :        0
   general:                 :        0

HSP details:
   hsp_operations           :    10441   hsp_sessio
```

Table 86 describes significant fields shown in the above display.

Table 86 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.
bytes before decomp	Number of compressed bytes that were presented to the compression algorithm from the input interface on decrypt.
bytes before comp	Number of uncompressed bytes (payload) that were presented to the compression algorithm from Cisco IOS on encrypt.
bytes after decomp	Number of decompressed bytes that were sent to Cisco IOS by the compression algorithm on decryption.
bytes after comp	Number of compressed bytes that were forwarded to Cisco IOS by the algorithm on encryption.
packets bypass compres	Number of packets that were not compressed because they were too small (<128 bytes).
packets not compressed	Number of packets that were not compressed because the packets were expanded rather than compressed.
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	Ratio of compression and decompression of packets presented to the compression algorithm, including those that were not compressed due to expansion or 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.

7200/VSA

The following example is output from a Cisco 7200 with VSA:

```
Router# show crypto engine accelerator statistic 0
Inbound rate: 0pps 0kb/s  Outbound rate: 0pps 0kb/s

    TRAFFIC                     Transmitted                 Received
 ------------------------------------------------------------------------------
  Message  Count:                       5                        5
  Message  Byte Count:               1212                      256
  Message  Overflow:                    0
  Outbound Count:                      54                      154
  Outbound Byte Count:              12472                    30332
  Outbound Overflow:                    0
  Inbound  Count:                     153                      153
  Inbound  Byte Count:              26304                    19864
  Inbound  Overflow:                    0

  Reassembled Pkt:                      0
  Fragments Dropped:                    0
     IPPE:                              0
     EPPE:                              0
```

```
     FIFO:                                0
     RAE:                                 0

  Inbound Traffic:
 ------------------------------------------------------------------------------
  Decrypted Pkt:                       150
  Passthrough Pkt:                       3
  IKE Pkt:                               0

  SPI Error:                             0
  Policy Violation:                      0

  Outbound Traffic:            Route cache                 Processor
 ------------------------------------------------------------------------------
  Encrypted Pkt:                       150                         0
  Passthrough Pkt:                       0                         4
  Policy Violation:                      0

  Queue Depth:
 ------------------------------------------------------------------------------
  TXRing Current Queue Depth:
    High Priority   :                    0.0 %
    Medium Priority :                    0.0 %
    Low Priority    :                    0.0 %

VSA RX Exception statistics:
   Invalid SA              :          0   Enc Dec mismatch        :          0
   Next Header mismatch    :          0   Pad mismatch            :          0
   MAC mismatch            :          0   Anti replay failed      :          0
   Enc Seq num overflow    :          0   Dec IPver mismatch      :          0
   Enc IPver mismatch      :          0   TTL Decr                :          0
   Selector checks         :          0   UDP mismatch            :          0
   IP Parse error          :          0   Fragmentation Error     :          0
   IB Selector check       :          0   TimeBased Replay Err    :          0
   Misc. Exceptions        :          0
```

Table 87 describes significant fields shown in the above display.

Table 87 show crypto engine statistic Field Descriptions for a Cisco 7200/VSA

Field	Description
Message Count	Number of messages sent to the VSA.
Message Byte Count	Byte count for the above messages.
Message Overflow	Number of messages that could not be sent because there was no space in the transmission (TX) ring.
Outbound Count	Number of outbound packets sent to the VSA for classification and/or encryption (includes packets for encryption/passthrough).
Outbound Byte Count	Byte count of the above packets.
Outbound Overflow	Number of outbound packets that could not be sent.
Inbound Count	Number of inbound packets sent to the VSA for classification and/or decryption.
Inbound Byte Count	Byte count for the above packets.

Table 87 show crypto engine statistic Field Descriptions for a Cisco 7200/VSA (continued)

Field	Description
Inbound Overflow	Number of inbound packets that could not be sent because the TX ring was full.
Reassembled Pkt	Number of reassembled packets.
Fragments Dropped	Total number of fragments dropped.
IPPE	Number of inbound fragments dropped by the Ingress Packet Processing Engine (IPPE)
EPPE	Number of outbound fragments dropped by the Egress Packet Processing Engine (EPPE).
FIFO	Number of fragments dropped by the FIFO (First In First Out) fragment queue.
RAE	Number of fragments dropped by the Reassembly Engine (RAE).
Inbound Traffic	
Decrypted Pkt	Number of decrypted packets.
Passthrough Pkt	Clear packets in the inbound direction.
IKE Pkt	Internet Key Exchange (IKE) packets that were received.
SPI Error	Received packets having an invalid Security Parameter Index (SPI).
Policy Violation	The VSA received clear packets that should have come encrypted as per the policy.
Outbound Traffic	
Encrypted Pkt	Number of encrypted packets.
Passthrough Pkt	Outbound clear packets.
Policy Violation	No outbound SA to encrypt the packet.
Queue Depth	
TXRing Current Queue Depth	Current queue depth of the three TX rings.
VSA RX Exception statistics	Errors from the crypto chip.
Invalid SA	Specified SA does not exist.
Enc Dec mismatch	Packet came on the wrong type of SA.
Next Header mismatch	Wrong nextheader field was found in the packet.
Pad mismatch	Wrong pad found in the packet.
MAC mismatch	Authentication check failed.
Anti replay failed	Anti-replay error.
Enc Seq num overflow	Sequence number reached the max for the SA.
Dec IPver mismatch	Wrong IP version for the packet to be decrypted (for example, an IPv4 packet came in for an IPv6 SA).

Table 87 show crypto engine statistic Field Descriptions for a Cisco 7200/VSA (continued)

Field	Description
Enc IPver mismatch	Wrong IP version for the packet to be encrypted. Wrong IP version for the packet to be encrypted.
TTL Decr	Time to Live decremented to 0 (zero).
Selector checks	Decrypted packet failed the policy check.
UDP mismatch	User Data Protocol (UDP) packet failed the sanity check.
IP Parse error	Error in IP packet parsing.
Fragmentation Error	Could not fragment; DF bit set.
IB Selector check	Decrypted packet failed the policy check (for Group Encrypted Transport Virtual Private Network [GET VPN]).
TimeBased Replay Err	Time-based anti-replay failed (for GET VPN).
Misc. Exceptions	Errors not classified as any of the above.

IPsec VPN SPA and VSPA

The following example shows the platform statistics for the IPsec VPN SPA in slot 1 subslot 0 and also displays the network interface controller statistics (this platform output is from a Catalyst 6500 series with installed IPsec VPN SPA):

```
Router# show crypto engine accelerator statistic slot 1/0 detail

VPN module in slot 1/0


Decryption Side Data Path Statistics
====================================
Packets RX..............: 454260
Packets TX..............: 452480

IPSec Transport Mode.....: 0
IPSec Tunnel Mode........: 452470
AH Packets..............: 0
ESP Packets..............: 452470
GRE Decapsulations.......: 0
NAT-T Decapsulations.....: 0
Clear....................: 8
ICMP.....................: 0

Packets Drop.............: 193
Authentication Errors....: 0
Decryption Errors........: 0
Replay Check Failed......: 0
Policy Check Failed......: 0
Illegal CLear Packet.....: 0
GRE Errors...............: 0
SPD Errors...............: 0
HA Standby Drop..........: 0

Hard Life Drop...........: 0
Invalid SA...............: 191
SPI No Match.............: 0
Destination No Match.....: 0
```

```
Protocol No Match........: 0

Reassembly Frag RX.......: 0
IPSec Fragments..........: 0
IPSec Reasm Done.........: 0
Clear Fragments..........: 0
Clear Reasm Done.........: 0
Datagrams Drop...........: 0
Fragments Drop...........: 0


Decryption Side Controller Statistics

====================================
Frames RX................: 756088
Bytes RX.................: 63535848
Mcast/Bcast Frames RX....: 2341
RX Less 128Bytes.........: 756025
RX Less 512Bytes.........: 58
RX Less 1KBytes..........: 2
RX Less 9KBytes..........: 3
RX Frames Drop...........: 0

Frames TX................: 452365
Bytes TX.................: 38001544
Mcast/Bcast Frames TX....: 9
TX Less 128Bytes.........: 452343
TX Less 512Bytes.........: 22
TX Less 1KBytes..........: 0
TX Less 9KBytes..........: 0


Encryption Side Data Path Statistics
====================================
Packets RX...............: 756344
Packets TX...............: 753880
IPSec Transport Mode.....: 0
IPSec Tunnel Mode........: 753869
GRE Encapsulations.......: 0
NAT-T Encapsulations.....: 0
LAF prefragmented........: 0

Fragmented...............: 0
Clear....................: 753904
ICMP.....................: 0

Packets Drop.............: 123
IKE/TED Drop.............: 27
Authentication Errors....: 0
Encryption Errors........: 0
HA Standby Drop..........: 0

Hard Life Drop...........: 0
Invalid SA...............: 191

Reassembly Frag RX.......: 0
Clear Fragments..........: 0
Clear Reasm Done.........: 0
Datagrams Drop...........: 0
Fragments Drop...........: 0


Encryption Side Controller Statistics
====================================
```

```
Frames RX.................: 454065
Bytes RX..................: 6168274/
Mcast/Bcast Frames RX....: 1586
RX Less 128Bytes.........: 1562
RX Less 512Bytes.........: 452503
RX Less 1KBytes..........: 0
RX Less 9KBytes..........: 0
RX Frames Drop...........: 0

Frames TX.................: 753558
Bytes TX..................: 100977246
Mcast/Bcast Frames TX....: 2
TX Less 128Bytes.........: 3
TX Less 512Bytes.........: 753555
TX Less 1KBytes..........: 0
TX Less 9KBytes..........: 0
```

Table 88 describes significant fields shown in the above display.

Table 88 show crypto engine accelerator statistic IPsec VPN SPA Statistics Descriptions

Field	Description
Decryption Data Side Path Statistics	
Packets RX	Number of packets received on the decryption side of the IPsec VPN SPA.
Packets TX	Number of packets transmitted by the IPsec VPN SPA in the decryption direction.
IPSec Transport Mode	Number of packets in IPsec Transport Mode.
IPSec Tunnel Mode	Number of packets in IPsec Tunnel Mode.
AH Packets	Number of packets with authentication headers (AHs).
ESP Packets	Number of packets with Encapsulating Security Payload (ESP) headers.
GRE Decapsulations	Number of packets that were generic routing encapsulating (GRE) decapsulated.
NAT-T Decapsulations	Number of packets that were Network Address Translation-Traversal (NAT-T) decapsulated.
Clear	Number of clear packets received.
ICMP	Number of Internet Control Message Protocol (ICMP) packets received.
Packets Drop	Number of packet drops. **Note** Does not represent the sum of the individual drop subtotals displayed (does not include BPDU/CDP/MOP packets dropped).
Authentication Errors	Number of authentication errors.
Decryption Errors	Number of decryption errors.
Replay Check Failed	Number of replay check errors.

Table 88 show crypto engine accelerator statistic IPsec VPN SPA Statistics Descriptions (continued)

Field	Description
Policy Check Failed	Number of policy check errors.
Illegal Clear Packet	Number of illegal clear packets.
GRE Errors	Number of GRE errors due to invalid packets or invalid security associations (SAs). **Note** These errors correspond to the sum of the following GRE errors in the output of the **show stats icpu** command: "GRE Packet Errors," "GRE SA No Match," and "Invalid GRE SA," which count, respectively, the number of GRE packets that are RFC compliant but that use a format currently not supported by the VPN module, the number of GRE packets in which the SA lookup results is a no match, and the number of GRE packets in which the SA lookup matches an entry marked as invalid.
SPD Errors	Number of Security Policy Database (SPD) errors. **Note** These errors correspond to the sum of the following SPD errors in the output of the **show stats icpu** command: "SPD Lookup Failed," "SPD Invalid," and "SPD ID No Match."
HA Standby Drop	Number of packet drops on a High Availability (HA) standby IPsec VPN SPA. **Note** The standby IPsec VPN SA is not supposed to receive packets.
Hard Life Drop	Number of packet drops due to SA hard life expiration. **Note** These packets are dropped during rekeying after the SA volume lifetime has been reached.
Invalid SA	Number of packet drops due to invalid SA.
SPI No Match	Number of packet drops due to a Security Parameter Index (SPI) mismatch.
Destination No Match	Number of packet drops due to destination no match.
Protocol No Match	Number of packet drops due to protocol no match.
Reassembly Frag RX	Number of packets that required reassembly processing.
IPSec Fragments	Number of IPsec fragments.

Table 88 show crypto engine accelerator statistic IPsec VPN SPA Statistics Descriptions (continued)

Field	Description
IPSec Reasm Done	Number of IPsec fragments reassembled.
Clear Fragments	Number of clear fragments.
Clear Reasm Done	Number of clear fragments reassembled.
Datagrams Drop	Number of reassembled datagrams dropped.
Fragments Drop	Number of fragments dropped.
Decryption Side Controller Statistics	
Frames RX	Number of frames received.
Bytes RX	Number of bytes received.
Mcast/Bcast Frames RX	Number of multicast/broadcast frames received.
RX Less 128Bytes	Number of frames having a size less than 128 bytes.
RX Less 512Bytes	Number of frames having a size greater than or equal to 128 bytes and less than 512 bytes.
RX Less 1KBytes	Number of frames having a size greater than or equal to 512 bytes and less than 1 kilobyte (KB).
RX Less 9KBytes	Number of frames having a size greater than or equal to 1 KB and less than 9 KBs.
RX Frames Drop	Number of frames dropped.
Frames TX	Number of frames transmitted.
Bytes TX	Number of bytes transmitted.
Mcast/Bcast Frames TX	Number of multicast/broadcast frames transmitted.
TX Less 128Bytes	Number of frames having a size less than 128 bytes.
TX Less 512Bytes	Number of frames having a size greater than or equal to 128 bytes and less than 512 bytes.
TX Less 1KBytes	Number of frames having a size greater than or equal to 512 bytes and less than 1 KB.
TX Less 9KBytes	Number of frames having a size greater than or equal to 1 KB and less than 9 KBs.
Encryption Side Data Path Statistics	
Packets RX	Number of packets received on the encryption side of the IPsec VPN SPA.
Packets TX	Number of packets transmitted by the IPsec VPN SPA in the encryption direction.
IPSec Transport Mode	Number of packets in IPsec Transport Mode.
IPSec Tunnel Mode	Number of packets in IPsec Tunnel Mode.
GRE Encapsulations	Number of packets that were GRE encapsulated.

Table 88 show crypto engine accelerator statistic IPsec VPN SPA Statistics Descriptions (continued)

Field	Description
NAT-T Encapsulations	Number of packets that were NAT-T encapsulated.
LAF prefragmented	Number of packets with Look Ahead Fragmentation set and that were prefragmented.
Fragmented	Number of packets fragmented.
Clear	Number of clear packets.
ICMP	Number of ICMP packets.
Packets Drop	Number of packet drops. **Note** Does not represent the sum of the individual drop subtotals displayed (does not include BPDU/CDP/MOP packets dropped).
IKE/TED Drop	Number of packet drops because SA has not been set up.
Authentication Errors	Number of authentication errors.
Encryption Errors	Number of Encryption errors.
HA Standby Drop	Number of packet drops on a HA standby IPsec VPN SPA. **Note** The standby IPsec VPN SPA is not supposed to receive packets.
Hard Life Drop	Number of packet drops due to SA hard-life expiration. **Note** These packets are dropped during rekeying after the SA volume lifetime has been reached.
Invalid SA	Number of packet drops due to invalid SA.
Reassembly Frag RX	Number of packets that required reassembly processing.
Clear Fragments	Number of clear fragments.
Clear Reasm Done	Number of clear fragments reassembled.
Datagrams Drop	Number of reassembled datagrams dropped.
Fragments Drop	Number of fragments dropped.
Encryption Side Controller Statistics	
Frames RX	Number of frames received.
Bytes RX	Number of bytes received.
Mcast/Bcast Frames RX	Number of multicast/broadcast frames received.
RX Less 128Bytes	Number of frames having a size less than 128 bytes.

Table 88 show crypto engine accelerator statistic IPsec VPN SPA Statistics Descriptions (continued)

Field	Description
RX Less 512Bytes	Number of frames having a size greater than or equal to 128 bytes and less than 512 bytes.
RX Less 1KBytes	Number of frames having a size greater than or equal to 512 bytes and less than 1 KB.
RX Less 9KBytes	Number of frames having a size greater than or equal to 1 KB and less than 9 KBs.
RX Frames Drop	Number of frames dropped.
Frames TX	Number of frames transmitted.
Bytes TX	Number of bytes transmitted.
Mcast/Bcast Frames TX	Number of multicast/broadcast frames transmitted.
TX Less 128Bytes	Number of frames having a size less than 128 bytes.
TX Less 512Bytes	Number of frames having a size greater than or equal to 128 bytes and less than 512 bytes.
TX Less 1KBytes	Number of frames having a size greater than or equal to 512 bytes and less than 1 KB.
TX Less 9KBytes	Number of frames having a size greater than or equal to 1 KB and less than 9 KBs.

VSPA

The following examples show the output when the **coreutil** keyword is used with the VSPA and the Catalyst 6500 series switch using Cisco IOS Release 12.2(33)SXI and later releases:

```
Router#: show crypto engine accelerator statistic slot 2/0 coreutil

Utilization Percentages for VPN blade in slot 2/0
Blade Utilization Percentages
=========================
Last 5 seconds --------------------
Slowpath ..................... 35 %
Inbound ...................... 24 %
Outbound ..................... 32 %
QoS .......................... 44 %
Last 1 minute ----------------------
Slowpath ..................... 12 %
Inbound ...................... 11 %
Outbound ..................... 15 %
QoS .......................... 23 %
Last 5 minutes ---------------------
Slowpath ...................... 8 %
Inbound ...................... 11 %
Outbound ..................... 11 %
QoS .......................... 10 %

Router# show crypto engine accelerator statistic all coreutil

Utilization Percentages for VPN blade in slot 2/0
Blade Utilization Percentages
```

```
==========================
Last 5 seconds ---------------------
Slowpath ..................... 35 %
Inbound ...................... 24 %
Outbound ..................... 32 %
QoS .......................... 44 %
Last 1 minute ----------------------
Slowpath ..................... 12 %
Inbound ...................... 11 %
Outbound ..................... 15 %
QoS .......................... 23 %
Last 5 minutes ---------------------
Slowpath ...................... 8 %
Inbound ...................... 11 %
Outbound ..................... 11 %
QoS .......................... 10 %
Utilization Percentages for VPN blade in slot 2/1
Blade Utilization Percentages
==========================
Last 5 seconds ---------------------
Slowpath ..................... 88 %
Inbound ...................... 78 %
Outbound ..................... 79 %
QoS .......................... 32 %
Last 1 minute ----------------------
Slowpath ..................... 76 %
Inbound ...................... 80 %
Outbound ..................... 80 %
QoS .......................... 13 %
Last 5 minutes ---------------------
Slowpath ..................... 75 %
Inbound ...................... 65 %
Outbound ..................... 70 %
QoS .......................... 12 %
```

Table 89 describes significant fields shown in the above display.

Table 89 show crypto engine accelerator statistic coreutil VSPA Statistics Descriptions

Field	Description
Blade Utilization Percentages	
Slowpath	Utilization of slowpath traffic capacity.
Inbound	Utilization of inbound traffic capacity.
Outbound	Utilization of outbound traffic capacity.
QoS	Utilization of QoS traffic capacity.

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.

Command	Description
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 gdoi

To display information about a Group Domain of Interpretation (GDOI) configuration, use the **show crypto gdoi** command in privileged EXEC mode.

show crypto gdoi [**debug-condition**] [**group** *group-name*] [**gm** [**acl** | **rekey** | **replay**] | **ks** [**acl** | **coop** [**version**] | **members** [*ip-address*] | **policy** | **rekey** | **replay**]] [**ipsec sa**]

Syntax Description

debug-condition	(Optional) Displays GDOI debug conditional filters.
group *group-name*	(Optional) Displays information about the group specified.
gm	(Optional) Displays information about group members.
acl	(Optional) Displays the access control list (ACL) that has been applied to the GDOI group.
rekey	(Optional) Displays rekey information.
replay	(Optional) Displays group information for time-based anti-replay.
ks	(Optional) Displays information about key servers.
coop	(Optional) Displays information about the cooperative key servers.
version	(Optional) Displays information about the cooperative key server and client versions.
members [*ip-address*]	(Optional) Displays information about registered group members.
policy	(Optional) Displays key server policy information.
ipsec sa	(Optional) Displays information about the IP security (IPsec) security association (SA) for all group members. • If this keyword is used with the **group** *group-name* keyword and argument option, information is displayed for only the group that is specified.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.4(11)T	The **group** *group-name* keyword and argument and **gm**, **acl**, **rekey**, **replay**, **ks**, **coop** [**version**], **members**, **policy**, and **ipsec sa** keywords were added.
Cisco IOS XE Release 2.3	This command was implemented on the Cisco ASR 1000 series routers.
15.1(3)T	This command was modified. The **debug-condition** keyword was added.

Usage Guidelines

Because the **show running-config** command does not display enabled debug commands, the **debug-condition** keyword is useful for displaying GDOI debug conditional filters that are enabled.

Examples

The following output displays information about a configuration for a GDOI group member:

```
Router# show crypto gdoi group diffint

Group Information
   Group Name                  : diffint
   Group Identity              : 3333
   Group Members Registered    : 0
   Group Server                : 10.0.5.2


   Group Name                  : test
   Group Identity              : 4444
   Group Members Registered    : 0
   Group Server                : 10.0.5.2
```

The following output displays information about a configuration when entered on a GDOI key server:

```
Router# show crypto gdoi group diffint ks

Group Information
   Group Name                  : diffint
   Group Identity              : 3333
   Group Members Registered    : 1
   Group Server                : Local
   Group Rekey Lifetime        : 300 secs
   Group Rekey
       Remaining Lifetime      : 84 secs
   IPSec SA Number             : 1
     IPSec SA Rekey Lifetime   : 120 secs
     Profile Name              : gdoi-p
   SA Rekey
       Remaining Lifetime      : 64 secs
   access-list 120 permit ip host 10.0.1.1 host 192.168.1.1
   access-list 120 permit ip host 10.0.100.2 host 192.168.1.1

   Group Member List for Group diffint :
   Member ID                   : 10.0.3.1

   Group Name                  : test
   Group Identity              : 4444
   Group Members Registered    : 0
   Group Server                : Local
   Group Rekey Lifetime        : 600 secs
   IPSec SA Number             : 1
     IPSec SA Rekey Lifetime   : 120 secs
     Profile Name              : gdoi-p
   access-list 120 permit ip host 10.0.1.1 host 192.168.1.1
   access-list 120 permit ip host 10.0.100.2 host 192.168.1.1
```

The following output displays GDOI key server information for registered GMs when entered on a GDOI key server:

```
Router# show crypto gdoi ks members

Group Member Information :

Detail :

Number of rekeys sent for group diffint : 10

Group Member ID   : 5.0.6.1
Group ID          : 3333
Group Name        : diffint
```

```
Key Server ID     : 5.0.10.1
Rekeys sent       : 10
Rekeys retries    : 0
Rekey Acks Rcvd   : 10
Rekey Acks missed : 0

Sent seq num :    2    3    1    2
Rcvd seq num :    2    3    1    2

Group Member ID   : 5.0.5.1
Group ID          : 3333
Group Name        : diffint
Key Server ID     : 5.0.8.1
Rekeys sent       : 10
Rekeys retries    : 0
Rekey Acks Rcvd   : 10
Rekey Acks missed : 0

Sent seq num :    2    3    1    2
Rcvd seq num :    2    0    0    0
```

show crypto ha

To display all virtual IP (VIP) addresses that are currently in use by IP Security (IPSec) and Internet Key Exchange (IKE), use the **show crypto ha** command in privileged EXEC mode.

show crypto ha

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(11)T	This command was introduced.

Examples

The following output from the **show crypto ha** command shows all VIP addresses that are being used by IPSec and IKE:

```
Router# show crypto ha

IKE VIP: 209.165.201.3
  stamp: 74 BA 70 27 9C 4F 7F 81 3A 70 13 C9 65 22 E7 76
IKE VIP: 255.255.255.253
  stamp: Not set
IKE VIP: 255.255.255.254
  stamp: Not set
IPSec VIP: 209.165.201.3
IPSec VIP: 255.255.255.253
IPSec VIP: 255.255.255.254
```

show crypto identity

To display the crypto identity list, use the **show crypto identity** command in privileged EXEC mode.

show crypto identity [*identity-tag*]

Syntax Description

identity-tag	(Optional) The crypto identity tag value for which to display specific crypto identity list information.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SRB	This command was introduced in a release earlier than Cisco IOS Release 12.2(33)SRB.
12.2SX	This command was integrated into Cisco IOS Release 12.2SX.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
Cisco IOS XE 2.3	This command was integrated into Cisco IOS XE Release 2.3.

Usage Guidelines

Use the **show crypto identity** command to display the configured crypto identity of a router.

Examples

The following are sample outputs from the **show crypto identity** command:

```
Router# show crypto identity id12

crypto identity id12:
   Description: line 22

Router# show crypto identity id11

crypto identity id11:
   fqdn line22

Router# show crypto identity

crypto identity tag12:
   Description: Linedescription
   fqdn fullyauthorisedone
```

Table 90 describes the significant fields shown in the display.

Table 90 show crypto identity Field Descriptions

Field	Description
Description	Line description.
fqdn	Fully qualified distinguished name identifier

show crypto ikev2 diagnose error

To display the current Internet Key Exchange Version 2 (IKEv2) exit path database, use the **show crypto ikev2 diagnose error** command in privileged EXEC mode.

show crypto ikev2 diagnose error [**count**]

Syntax Description

count	(Optional) Display the error counters from the exit path database.

Command Default

The IKEv2 exit path database is displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(1)T	This command was introduced.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.

Usage Guidelines

Use this command to display the IKEv2 exit path database. Enable or disable IKEv2 exit path logging using the **crypto ikev2 diagnose error** command. Use the **clear crypto ikev2 diagnose error** command to clear the IKEv2 exit path database.

Examples

The following example is a sample output from the **show crypto ikev2 diagnose error** command. The output is self-explanatory.

```
Router# show crypto ikev2 diagnose error
Exit Path Table - status: enable, current entry 2, deleted 0, max allow 50

Error(1): No pskey found
 -Traceback= 0x37ABEB8z 0x37AC29Cz 0x2C0CA74z 0x2C0CA70z

Error(1): No pskey found
 -Traceback= 0x37B609Cz 0x37ABEB8z 0x37AC29Cz 0x2C0CA74z 0x2C0CA70z
```

Related Commands

Command	Description
clear crypto ikev2 diagnose error	Clears the IKEv2 exit path database.
crypto ikev2 diagnose error	Enables IKEv2 error diagnosis.

show crypto ikev2 policy

To display the default or a user-defined Internet Key Exchange Version 2 (IKEv2) policy, use the **show crypto ikev2 policy** command in privileged EXEC mode.

show crypto ikev2 policy [*policy-name*]

Syntax Description

policy-name	(Optional) Displays the specified policy.

Command Default

If no option is specified, then this command displays all the policies.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(1)T	This command was introduced.
15.1(4)M	This command was modified. The command output was updated to support IPv6 addresses.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.

Usage Guidelines

Use this command to display the default or user-defined IKEv2 policy. User-defined policies display the default values of the commands that are not explicitly configured under the policy.

Examples

The following examples show the output for a default and user-defined policy.

Default IKEv2 Policy

The default IKEv2 policy matches all local addresses in global VRF and uses the default IKEv2 proposal.

```
Router# show crypto ikev2 policy default

 IKEv2 policy : default
      Match fvrf  : global
      Match address local : any
      Proposal    : default

Router# show crypto ikev2 policy default
```

This sample output shows the default IKEv2 policy that matches the local IPv6 address in global VRF:
IKEv2 policy : default

```
      Match fvrf  : global
      Match address local : 2001:DB8:1::1
      Proposal    : default
```

User-defined IKEv2 policy

```
Router# show crypto ikev2 policy policy-1

    IKEv2 policy : policy-1
        Match fvrf : green
        Match local : 10.0.0.1
        Proposal    : proposal-A
        Proposal    : proposal-B
```

Table 91 describes the significant fields shown in the display.

Table 91 show crypto ikev2 policy Field Descriptions

Field	Description
IKEv2 policy	Name of the IKEv2 policy.
Match fvrf	The front door virtual routing and forwarding (FVRF) specified for matching the IKEv2 policy.
Match local	The local IP address (IPv4 or IPv6) assigned for matching the IKEv2 policy.
Proposal	The name of the proposal that is attached to the IKEv2 policy.

Related Commands

Command	Description
crypto ikev2 policy	Defines an IKEv2 policy.
crypto ikev2 proposal	Defines an IKE proposal.
match (ikev2 policy)	Matches an IKEv2 policy based on the parameters.
proposal	Specifies the proposals that must be used in the IKEv2 policy.

show crypto ikev2 profile

To display a user-defined Internet Key Exchange Version 2 (IKEv2) profile, use the **show crypto ikev2 profile** command in privileged EXEC mode.

show crypto ikev2 profile [*profile-name*]

Syntax Description

profile-name	(Optional) Name of the IKEv2 profile.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(1)T	This command was introduced.
15.1(4)M	This command was modified. The command output was updated to support IPv6 addresses.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.

Usage Guidelines

Use this command to display information about an IKEv2 profile. This command also displays the default values of the commands that are not explicitly configured in the IKEv2 profile. If a profile name is not specified, the command displays all the user-defined IKEv2 profiles.

Examples

The following example is sample output from the **show crypto ikev2 profile** command:

```
Router# show crypto ikev2 profile

IKEv2 profile: prof
 Ref Count: 3
 Match criteria:
  Fvrf: any
  Local address/interface: none
  Identities:
   fqdn smap-initiator
  Certificate maps: none
 Local identity: fqdn dmap-responder
 Remote identity: none
 Local authentication method: pre-share
 Remote authentication method(s): pre-share
 Keyring: v2-kr1
 Trustpoint(s): none
 Lifetime: 86400 seconds
 DPD: disabled
 NAT-keepalive: disabled
 Ivrf: global
```

```
Virtual-template: none
Accounting mlist: none
```

Table 92 describes the significant fields shown in the display.

Table 92 show crypto ikev2 profile Field Descriptions

Field	Description
IKEv2 profile	Name of the IKEv2 profile.
Match	The match parameter in the profile.
Local Identity	The local identity type.
Local authentication method	The local authentication methods.
Remote authentication method	The remote authentication methods.
Keyring	The keyring specified in the profile.
Trustpoint	The trustpoints used in the Rivest, Shamir and Adleman (RSA) signature authentication method.
Lifetime	The lifetime of the IKEv2 profile.
DPD	The status of Dead Peer Detection (DPD).
Ivrf	The Inside VRF (IVRF) in the profile.
Virtual-template	The virtual template in the profile.

show crypto ikev2 proposal

To display the Internet Key Exchange Version 2 (IKEv2) proposal, use the **show crypto ikev2 proposal** command in privileged EXEC mode.

show crypto ikev2 proposal [*name* | *default*]

Syntax Description

name	(Optional) The user-defined proposal.
default	(Optional) The default proposal.

Command Default

If no option is specified, the default and user-defined proposals are displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(1)T	This command was introduced.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.

Usage Guidelines

Use this command to display the user-defined and default proposals.

Examples

The following example is a sample output from the **show crypto ikev2 proposal** command:

```
Router# show crypto ikev2 proposal

 IKEv2 proposal: pr1
     Encryption : 3DES AES-CBC-192
     Integrity  : MD596
     PRF        : MD5
     DH Group   : DH_GROUP_768_MODP/Group 1 DH_GROUP_1536_MODP/Group 5
 IKEv2 proposal: default
     Encryption : AES-CBC-128 3DES
     Integrity  : SHA96 MD596
     PRF        : SHA1 MD5
     DH Group   : DH_GROUP_1536_MODP/Group 5 DH_GROUP_1024_MODP/Group 2
```

Table 93 describes the significant fields shown in the display.

Table 93 show crypto ikev2 proposal Field Descriptions

Field	Description
IKEv2 proposal	Name of the proposal.
Encryption	The encryption algorithm configured in the proposal.
Integrity	The integrity algorithm configured in the proposal.

Table 93 show crypto ikev2 proposal Field Descriptions (continued)

Field	Description
PRF	The Pseudo-Random Function in the proposal. This is the same as the integrity algorithm.
DH Group	The Diffie-Hellman groups configured in the proposal.

Related Commands

Command	Description
crypto ikev2 proposal	Defines an IKEv2 proposal.
encryption (ikev2 proposal)	Specifies the encryption algorithm in an IKEv2 proposal.
group (ikev2 proposal)	Specifies the DH groups in an IKEv2 proposal.
integrity (ikev2 proposal)	Specifies the integrity algorithm in an IKEv2 proposal.

show crypto ikev2 sa

To display the Internet Key Exchange Version 2 (IKEv2) security associations (SA), use the **show crypto ikev2 sa** command in privileged EXEC mode.

show crypto ikev2 sa {**local** *ip-address* | **remote** *ip-address* | **fvrf** *vrf-name*} [**detailed**]

Syntax Description

local *ip-address*	Displays the current IKEv2 security associations matching the local address.
remote *ip-address*	Displays the current IKEv2 security associations matching the remote address.
fvrf *vrf-name*	Displays the current IKEv2 security associations matching the specified front door virtual routing and forwarding (FVRF).
detailed	(Optional) Displays detailed information about the current security associations.

Command Default

All the current IKEv2 security associations are displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(1)T	This command was introduced.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.

Usage Guidelines

Use this command to display information about the current IKEv2 security associations.

Examples

The following is sample output from the **show crypto ikev2 sa** command:

```
Router# show crypto ikev2 sa

Tunnel-id   Local          Remote           fvrf/ivrf          Status
2           10.0.0.1/500    10.0.0.2/500      (none)/(none)      READY
      Encr: 3DES, Hash: SHA96, DH Grp:2, Auth: PSK
      Life/Active Time: 86400/361 sec
```

The following is sample output from the **show crypto ikev2 sa detailed** command:

```
Router# show crypto ikev2 sa detailed

Tunnel-id Local                Remote                fvrf/ivrf            Status
1         1.1.1.1/500          1.1.1.2/500           (none)/(none)        READY
      Encr: 3DES, Hash: MD596, DH Grp:2, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/12 sec
      CE id: 1001, Session-id: 1
      Status Description: Negotiation done
      Local spi: 41E942F807BA4153       Remote spi: 993043F2AF648C48
```

```
Local id: 1.1.1.1
Remote id: 1.1.1.2
Local req msg id:  2              Remote req msg id:  0
Local next msg id: 2              Remote next msg id: 0
Local req queued:  2              Remote req queued:  0
Local window:      5              Remote window:      5
DPD configured for 0 seconds, retry 0
NAT-T is not detected
```

Table 94 describes the significant fields shown in the display.

Table 94 show crypto ikev2 sa detailed Field Descriptions

Field	Description
Tunnel-id	Unique identifier of the IKEv2 tunnel.
Local	IP address and UDP port of the local IKEv2 endpoint.
Remote	IP address and UDP port of the remote IKEv2 endpoint.
fvrf/ivrf	FVRF/IVRF of the local IKEv2 endpoint.
Status	Status of the IKEv2 tunnel.
Encr	Encryption algorithm used by the IKEv2 tunnel.
Hash	Integrity algorithm used by the IKEv2 tunnel.
DH Grp	Diffie-Hellman (DH) group used by the IKEv2 tunnel.
Auth Sign	Authentication method used by the local IKEv2 endpoint.
Auth Verify	Authentication method used by the remote IKEv2 endpoint.
Life/Active Time	The total and active lifetime of the IKEv2 tunnel.
CE id	The crypto engine ID used by the local IKEv2 endpoint.
Session-id	The session ID for the IKEv2 tunnel.
MIB-id	The MIB identifier for the IKEv2 tunnel.
Status Description	Description of the IKEv2 tunnel status.
Local spi	IKEv2 security parameter index (SPI) of the local IKEv2 endpoint.
Remote spi	IKEv2 SPI of the remote IKEv2 endpoint.
Local id	IKEv2 identity of the local IKEv2 endpoint
Remote id	IKEv2 identity of the remote IKEv2 endpoint.
Local req mess id	Message ID of the last IKEv2 request sent.
Remote req mess id	Message ID of the last IKEv2 request received.
Local next mess id	Message ID of the next IKEv2 request to be sent.
Remote next mess id	Message ID of the next IKEv2 request to be received.
Local req queued	Number of requests queued to be sent.
Remote req queued	Number of requests queued to be processed.
Local window	IKEv2 window size of the local IKEv2 endpoint.
Remote window	IKEv2 window size of the remote IKEv2 endpoint.

Table 94 show crypto ikev2 sa detailed Field Descriptions (continued)

Field	Description
DPD	DPD interval.
NAT-T	NAT detection status.

show crypto ikev2 session

To display the status of active Internet Key Exchange Version 2 (IKEv2) sessions, use the **show crypto ikev2 session** command in privileged EXEC mode.

show crypto ikev2 session [**detailed**]

Syntax Description

detailed	(Optional) Displays detailed information about the session.

Command Default

The session information is displayed in a brief format.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(1)T	This command was introduced.
15.1(4)M	This command was modified. The command output was updated to support IPv6 addresses.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.

Usage Guidelines

Use this command to display information about the active IKEv2 sessions. Use the **detailed** keyword to display information about IKEv2 parent and child security associations.

Examples

The following is a sample output from the **show crypto ikev2 session** and **show crypto ikev2 session detailed** command.

```
Router# show crypto ikev2 session

Session-id:1, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id   Local           Remote           fvrf/ivrf          Status
1           10.0.0.1/500     10.0.0.2/500      (none)/(none)      READY
      Encr: 3DES, Hash: SHA96, DH Grp:2, Auth: PSK
      Life/Active Time: 86400/65 sec
CHild sa: local selector  10.0.0.1/0 - 10.0.0.1/65535
          remote selector 10.0.0.2/0 - 10.0.0.2/65535
          ESP spi in/out: 0x9360A95/0x6C340600
          CPI in/out: 0x9FE5/0xC776

Router# show crypto ikev2 session detailed

Session-id:1, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id   Local          Remote           fvrf/ivrf          Status
1           10.0.0.1/500    10.0.0.2/500      (none)/(none)      READY
      Encr: 3DES, Hash: SHA96, DH Grp:2, Auth: PSK
```

```
      Life/Remaining/Active Time: 86400/86157/248 sec
      CE id: 0, Session-id: 1, MIB-id: 1
      Status Description: Negotiation done
      Local spi: 750CBE827434A245       Remote spi: 4353FEDBABEBF24C
      Local id:          10.0.0.1        Remote id:          10.0.0.2
      Local req mess id:    0           Remote req mess id: 0
      Local next mess id:    0          Remote next mess id: 2
      Local req queued:    0            Remote req queued: 0
      Local window:    5                 Remote window: 5
      DPD configured for 0 seconds
      NAT-T is not detected
Child sa: local selector  10.0.0.1/0 - 10.0.0.1/65535
          remote selector 10.0.0.2/0 - 10.0.0.2/65535
          ESP spi in/out: 0x9360A95/0x6C340600
          CPI in/out: 0x9FE5/0xC776
          AH spi in/out: 0x0/0x0
          Encr: AES CBC, keysize: 128, esp_hmac: SHA96
          ah_hmac: Unknown - 0, comp: IPCOMP_LZS, mode tunnel
```

Table 95 describes the significant fields shown in the display.

Table 95 show crypto ikev2 session detailed Field Descriptions

Field	Description
Tunnel id	Unique identifier of IKEv2 tunnel.
Local	IP address (IPv4 or IPv6) and UDP port of the local IKEv2 endpoint.
Remote	IPv4 or IPv6 address and UDP port of the remote IKEv2 endpoint.
fvrf/ivrf	FVRF/IVRF of the local IKEv2 endpoint.
Status	Status of the IKEv2 tunnel.
Encr	Encryption algorithm used by the IKEv2 tunnel.
Hash	Integrity algorithm used by the IKEv2 tunnel.
DH Grp	DH group used by the IKEv2 tunnel.
Auth Sign	Authentication method used by the local IKEv2 endpoint.
Auth Verify	Authentication method used by the remote IKEv2 endpoint.
Life/Active Time	The total and active lifetime of the IKEv2 tunnel.
CE id	The crypto engine ID used by the local IKEv2 endpoint.
Session-id	The session ID for the IKEv2 tunnel.
MIB-id	The MIB identifier for the IKEv2 tunnel.
Status Description	Description of the IKEv2 tunnel status.
Local spi	IKEv2 security parameter index (SPI) of the local IKEv2 endpoint.
Remote spi	IKEv2 SPI of the remote IKEv2 endpoint.
Local id	IKEv2 identity of the local IKEv2 endpoint
Remote id	IKEv2 identity of the remote IKEv2 endpoint.
Local req mess id	Message ID of the last IKEv2 request sent.
Remote req mess id	Message ID of the last IKEv2 request received.

Table 95 show crypto ikev2 session detailed Field Descriptions (continued)

Field	Description
Local next mess id	Message ID of the next IKEv2 request to be sent.
Remote next mess id	Message ID of the next IKEv2 request to be received.
Local req queued	Number of requests queued to be sent.
Remote req queued	Number of requests queued to be processed.
Local window	IKEv2 window size of the local IKEv2 endpoint.
Remote window	IKEv2 window size of the remote IKEv2 endpoint.
DPD	DPD interval.
NAT	NAT detection status.
Child sa: local selector	Local network protected by the child security association (SA).
remote selector	Remote network protected by the child SA.
ESP spi in/out	Inbound and outbound SPI of the Encapsulating Security Payload (ESP) child SA.
CPI in/out	Inbound and outbound Cisco Product Identification (CPI) of the IP compression (IPComp) child SA.
AH spi in/out	Inbound and outbound SPI of the Authentication Header (AH) child SA.
Encr	Encryption algorithm used by the ESP child SA.
keysize	Size of the key in bits used by the encryption algorithm.
esp_hmac	Integrity algorithm used by the ESP child SA.
ah_hmac	Integrity algorithm used in the AH child SA, if available.
comp	Compression algorithm used by IPComp child SA.
mode	Tunnel or transport mode used by ESP/AH child SA.

show crypto ikev2 stats

To display the Internet Key Exchange Version 2 (IKEv2) security associations (SAs) statistics, use the **show crypto ikev2 stats** command in privileged EXEC mode.

show crypto ikev2 stats

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(1)T	This command was introduced.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.

Usage Guidelines

Use this command to display IKEv2 security associations statistics.

Examples

The following example is a sample output from the **show crypto ikev2 stats** command. The fields in the output are self-explanatory.

```
Router(#) show crypto ikev2 stats
------------------------------------------------------------------------
              Crypto IKEV2 SA Statistics
------------------------------------------------------------------------
System Resource Limit:   0        Max IKEv2 SAs: 0        Max in nego: 1000
Total IKEv2 SA Count:    1        active:        1        negotiating: 0
Incoming IKEv2 Requests: 0        accepted:      0        rejected:    0
Outgoing IKEv2 Requests: 1        accepted:      1        rejected:    0
Rejected IKEv2 Requests: 0        rsrc low:      0        SA limit:    0
IKEv2 packets dropped at dispatch: 0
Incoming IKEV2 Cookie Challenged Requests: 0
    accepted: 0        rejected: 0        rejected no cookie: 0
```

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.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS 12.2SX family of releases. Support in a specific 12.2SX release is dependent on your feature set, platform, and platform hardware.

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. The last two lines indicate that a configuration URL and configuration version number have been pushed through the Mode-Configuration Exchange by the server to the Easy VPN remote device.

```
Router# show crypto ipsec client ezvpn

Tunnel name: hw1
Inside interface list: FastEthernet0/0, Serial1/0,
Outside interface: Serial0/0
Current State: IPSEC_ACTIVE
Last Event: SOCKET_UP
Address: 192.168.201.0
Mask: 255.255.255.224
DNS Primary: 192.168.201.1
DNS Secondary: 192.168.201.2
NBMS/WINS Primary: 192.168.201.3
NBMS/WINS Secondary: 192.168.201.4
Default Domain: cisco.com
Configuration URL: http://10.8.8.88/easy.cfg
Configuration Version: 10
```

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, Serial1/0,
```

```
Outside interface: Serial0/0
Current State: IPSEC_ACTIVE
Last Event: SOCKET_UP
Address: 192.168.202.128
Mask: 255.255.255.224
Default Domain: cisco.com

Split Tunnel List: 1
       Address    : 192.168.200.225
       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#
```

The following example displays information about the outside interface “Virtual-Access1”, which is bound to the real interface (Ethernet0/0) on which the user has configured Easy VPN as an outside interface:

```
Router# show crypto ipsec client ezvpn

Easy VPN Remote Phase: 5
Tunnel name : ez
Inside interface list: Ethernet1/0,
Outside interface: Virtual-Access1 (bound to Ethernet0/0)
Easy VPN connect ACL checking active
Connect : ACL based with access-list 101
Current State: CONNECT_REQUIRED
Last Event: TRACKED OBJECT UP
Save Password: Disallowed
Current EzVPN Peer: 10.0.0.2
```

Table 96 describes significant fields shown by the **show crypto ipsec client ezvpn** command:

Table 96 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.

Table 96 show crypto ipsec client ezvpn Field Descriptions (continued)

Field	Description
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 default transform-set

To display the default IP Security (IPsec) transform sets currently in use by Internet Key Exchange (IKE), use the **show crypto ipsec default transform-set** command in privileged EXEC mode.

show crypto ipsec default transform-set

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(20)T	This command was introduced.
Cisco IOS XE Release 2.4	This command was implemented on the Cisco ASR 1000 series routers.

Usage Guidelines

If the default transform sets are in use, the **show crypto ipsec default transform-set** command displays the two default transform sets each of which defines an Encapsulation Security Protocol (ESP) encryption transform type and an ESP authentication transform type.

Examples

The following example displays the two default transform sets. No user defined transform sets have been configured, the default transform sets have not been disabled, and the crypto engine supports the encryption algorithm.

```
Router# show crypto ipsec default transform-set

Transform set #$!default_transform_set_1: { esp-aes esp-sha-hmac  }
   will negotiate = { Transport,  },

Transform set #$!default_transform_set_0: { esp-3des esp-sha-hmac  }
   will negotiate = { Transport,  },
```

Table 97 show crypto ipsec default transform-set Field Descriptions

Default Transform Name	ESP Encryption Transform and Description	ESP Authentication Transform and Description
#$!default_transform_set_1	esp-aes (ESP with the 128-bit Advanced Encryption Standard [AES] encryption algorithm)	esp-sha-hmac (ESP with the Secure Hash Algorithm [SHA-1, HMAC variant] authentication algorithm)
#$!default_transform_set_0	esp-3des (ESP with the 168-bit Triple Data Encryption Standard [3DES or Triple DES] encryption algorithm)	esp-sha-hmac

The following example shows that when the default transform sets are disabled with the **no crypto ipsec default transform-set**, the **show crypto ipsec default transform-set** has no output.

```
Router(config)# no crypto ipsec default transform-set
Router(config)# exit
Router#
Router# show crypto ipsec default transform-set

Router#
```

Related Commands

Command	Description
crypto ipsec transform-set	Defines a transform set.
show crypto ipsec transform-set	Displays the configured transform sets.
show crypto map (IPsec)	Displays the crypto map configuration.

show crypto ipsec sa

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

show crypto ipsec sa [**map** *map-name* | **address** | **identity** | **interface** *type number* | **peer** [**vrf** *fvrf-name*] **address** | **vrf** *ivrf-name* | **ipv6** [**interface** *type number*]] [**detail**]

IPsec and IKE Stateful Failover Syntax

show crypto ipsec sa [**active** | **standby**]

Syntax Description

map *map-name*	(Optional) Displays any existing SAs that were created for the crypto map set with the value for the *map-name* argument.
address	(Optional) Displays all existing SAs, 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) Displays only the flow information. SA information is not shown.
interface *type number*	(Optional) Displays all existing SAs created for the interface value provided in the *interface* argument.
peer [**vrf** *fvrf-name*] **address**	(Optional) Displays all existing SAs with the peer address. If the peer address is in the Virtual Routing and Forwarding (VRF), specify **vrf** and the *fvrf-name*.
vrf *ivrf-name*	(Optional) Displays all existing SAs whose inside virtual routing and forwarding (IVRF) is the same as the valued used for the *ivrf-name* argument.
ipv6	(Optional) Displays IPv6 crypto IPsec SAs.
detail	(Optional) Detailed error counters. (The default is the high-level send or receive error counters.)
active	(Optional) Displays high availability (HA) - enabled IPsec SAs that are in the active state.
standby	(Optional) Displays HA-enabled IPsec SAs that are in the standby state.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.3T	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.

Release	Modification
12.2(15)T	The **interface** keyword and *type* and *number* arguments were added. The **peer** keyword, the **vrf** keyword, and the *fvrf-name* argument were added. The **address** keyword was added to the **peer** keyword string. The **vrf** keyword and *ivrf-name* argument were added.
12.3(11)T	The **active** and **standby** keywords were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.(33)SRA.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.1	This command was modified. This command was implemented on the Cisco ASR 1000 Series Aggregation Services Routers.

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 from the **show crypto ipsec sa** command:

```
Router# show crypto ipsec sa

interface: Tunnel1
    Crypto map tag: Tunnel1-head-0, local addr 10.5.5.2
   protected vrf: (none)
   local  ident (addr/mask/prot/port): (10.5.5.2/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (10.5.5.1/255.255.255.255/47/0)
   current_peer 10.5.5.1 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 492908510, #pkts encrypt: 492908510, #pkts digest: 492908510
    #pkts decaps: 492908408, #pkts decrypt: 492908408, #pkts verify: 492908408
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 55, #recv errors 0

     local crypto endpt.: 10.5.5.2, remote crypto endpt.: 10.5.5.1
     path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/2
     current outbound spi: 0xDE4EE29D(3729711773)

     inbound esp sas:
       spi: 0xC06CA92B(3228346667)
         transform: esp-3des esp-sha-hmac ,
         in use settings ={Tunnel, }
         conn id: 3139, flow_id: VSA:1139, crypto map: Tunnel1-head-0
         sa timing: remaining key lifetime (k/sec): (3948785/556)
         IV size: 8 bytes
         replay detection support: Y
         Status: ACTIVE

     inbound ah sas:
       spi: 0xC87AB936(3363486006)
         transform: ah-md5-hmac ,
         in use settings ={Tunnel, }
```

```
        conn id: 3139, flow_id: VSA:1139, crypto map: Tunnel1-head-0
        sa timing: remaining key lifetime (k/sec): (3948785/556)
        replay detection support: Y
        Status: ACTIVE

    inbound pcp sas:

    outbound esp sas:
      spi: 0xDE4EE29D(3729711773)
        transform: esp-3des esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 3140, flow_id: VSA:1140, crypto map: Tunnel1-head-0
        sa timing: remaining key lifetime (k/sec): (3948785/556)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE

    outbound ah sas:
      spi: 0xAEEDD4F1(2934822129)
        transform: ah-md5-hmac ,
        in use settings ={Tunnel, }
        conn id: 3140, flow_id: VSA:1140, crypto map: Tunnel1-head-0
        sa timing: remaining key lifetime (k/sec): (3948785/556)
        replay detection support: Y
        Status: ACTIVE

    outbound pcp sas:
```

The following is sample output from the **show crypto ipsec sa identity detail** command:

```
Router# show crypto ipsec sa identity detail

interface: Tunnel1
    Crypto map tag: Tunnel1-head-0, local addr 10.5.5.2
   protected vrf: (none)
   local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   current_peer (none) port 500
     DENY, flags={ident_is_root,}
     #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
     #pkts no sa (send) 0, #pkts invalid sa (rcv) 0
     #pkts encaps failed (send) 0, #pkts decaps failed (rcv) 0
     #pkts invalid prot (recv) 0, #pkts verify failed: 0
     #pkts invalid identity (recv) 0, #pkts invalid len (rcv) 0
     #pkts replay rollover (send): 0, #pkts replay rollover (rcv) 0
     ##pkts replay failed (rcv): 0
     #pkts internal err (send): 0, #pkts internal err (recv) 0

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (10.5.5.2/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (10.5.5.1/255.255.255.255/47/0)
   current_peer 10.5.5.1 port 500
     PERMIT, flags={origin_is_acl,}
     #pkts encaps: 492923510, #pkts encrypt: 492923510, #pkts digest: 492923510
     #pkts decaps: 492923408, #pkts decrypt: 492923408, #pkts verify: 492923408
     #pkts compressed: 0, #pkts decompressed: 0
     #pkts not compressed: 0, #pkts compr. failed: 0
     #pkts not decompressed: 0, #pkts decompress failed: 0
     #pkts no sa (send) 55, #pkts invalid sa (rcv) 0
     #pkts encaps failed (send) 0, #pkts decaps failed (rcv) 0
```

```
#pkts invalid prot (recv) 0, #pkts verify failed: 0
#pkts invalid identity (recv) 0, #pkts invalid len (rcv) 0
#pkts replay rollover (send): 0, #pkts replay rollover (rcv) 0
##pkts replay failed (rcv): 0
#pkts internal err (send): 0, #pkts internal err (recv) 0
```

Table 98 describes the significant fields shown in the above displays (**show crypto ipsec sa** and **show crypto ipsec sa detail**).

Table 98 show crypto ipsec sa Field Descriptions

Field	Description
crypto map tag	Policy tag for IPsec.
protected vrf	IVRF name that applies to the IPsec interface.
local ident (addr/mask/prot/port)	Local selector that is used for encryption and decryption.
remote ident (addr/mask/prot/port)	Remote selector that is used for encryption and decryption.
current peer	Current peer with which the IPsec tunnel communicates.
PERMIT, flags	IPsec SA is triggered by the Access Control List (ACL) permit action.
pkts encaps	Statistics number of packets that were successfully encapsulated by IPsec.
pkts encrypt	Statistics number of packets that were successfully encrypted by IPsec.
pkts digest	Statistics number of packets that were successfully hash digested by IPsec.
pkts decaps	Statistics number of packets that were successfully decapsulated by IPsec.
pkts decrypt	Statistics number of packets that were successfully decrypted by IPsec.
pkts verify	Received packets that passed the hash digest check.
pkts compressed	Number of packets that were successfully compressed by IPsec.
pkts decompressed	Number of packets that were successfully decompressed by IPsec.
pkts not compressed	Number of outbound packets that were not compressed.
pkts compr. failed	Number of packets that failed compression by IPsec.
pkts not decompressed	Number of inbound packets that were not compressed.
pkts decompress failed	Number of packets that failed decompression by IPsec.
send errors	Number of outbound packets that had errors.
recv errors	Number of inbound packets that had errors.
local crypto endpt.	Local endpoint terminated by IPsec.
remote crypto endpt.	Remote endpoint terminated by IPsec.

Table 98 show crypto ipsec sa Field Descriptions

Field	Description
path mtu	Maximum transmission unit (MTU) size that is figured based on the Internet Control Message Protocol (ICMP) unreachable packet. This value also has to consider the IPsec overhead.
ip mtu	Interface MTU size that considers the IPsec overhead.
current outbound spi	Current outbound Security Parameters Index (SPI).
ip mtu idb	Interface description block (IDB) that is used to determine the crypto IP MTU.
current outbound spi	Current outbound Security Parameter Index (SPI).
inbound esp sas	Encapsulating Security Payload (ESP) for the SA for the inbound traffic.
spi	SPI for classifying the inbound packet.
transform	Security algorithm that is used to provide authentication, integrity, and confidentiality.
in use settings	Transform that the SA uses (for example: tunnel mode, transport mode, UDP-encapsulated tunnel mode, or UDP-encapsulated transport mode).
conn id	ID that is stored in the crypto engine to identify the IPsec/Internet Key Exchange (IKE) SA.
flow_id	SA identity.
crypto map	Policy for the IPsec.
sa timing: remaining key lifetime (k/sec)	Seconds or kilobytes remaining before a rekey occurs.
IV size	Size of the initialization vector that is used for the cryptographic synchronization data used to encrypt the payload.
replay detection support	A specific SA has enabled the replay detection feature.
inbound ah sas	Authentication algorithm for the SA for inbound traffic.
inbound pcp sas	Compression algorithm for the SA for inbound traffic.
outbound esp sas	Encapsulating security payload for the SA for outbound traffic.
outbound ah sas	Authentication algorithm for the SA for outbound traffic.
outbound pcp sas	Compression algorithm for the SA for outbound traffic.
DENY, flags	IPsec SA is triggered by the ACL deny action.
pkts decompress failed	Number of packets decompressed by IPsec that failed.
pkts no sa (send)	Outbound packets cannot find the associated IPsec SA.
pkts invalid sa (rcv)	Received packets that failed the IPsec format check.
pkts invalid prot (recv)	Received packets that have the wrong protocol field.
pkts verify failed	Received packets that failed the hash digest check.

Table 98 show crypto ipsec sa Field Descriptions

Field	Description
pkts invalid identity (recv)	Packets after decryption cannot find the associated selector.
pkts pkts invalid len (rcv)	For the software crypto engine, inbound packets that have an incorrect pad length.
pkts replay rollover (send)	Sent packets that failed the replay test check.
pkts replay rollover (rcv)	Received packets that failed the replay test check.
pkts internal err (send)	Sent packets that failed because of a software or hardware error.
pkts internal err (rcv)	Received packets that failed because of a software or hardware error.
protected vrf	IVRF name that applies to the IPsec interface.

show crypto ipsec sa vrf Command Output

The following is sample output from the **show crypto ipsec sa vrf** 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 preceding **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
```

Table 99 describes the significant fields shown in the preceding **show crypto ipsec sa vrf** display. Additional fields are self-explanatory or can be found in Table 98.

Table 99 show crypto ipsec sa vrf Field Descriptions

Field	Description
remote crypto endpt.	Remote endpoint terminated by IPsec.
media mtu	MTU value for media, such as an Ethernet or a serial interface.
inbound esp sas	Encapsulating security payload for the SA of the inbound traffic.

IPsec and IKE Stateful Failover Examples

The following sample output shows the IPsec SA status of only the active device:

```
Router# show crypto ipsec sa active

interface: Ethernet0/0
    Crypto map tag: to-peer-outside, local addr 10.165.201.3

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.0.1/255.255.255.255/0/0)
   remote ident (addr/mask/prot/port): (172.16.0.1/255.255.255.255/0/0)
   current_peer 209.165.200.225 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 3, #pkts encrypt: 3, #pkts digest: 3
    #pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
    #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.: 209.165.201.3, remote crypto endpt.: 209.165.200.225
     path mtu 1500, media mtu 1500
```

```
    current outbound spi: 0xD42904F0(3559458032)

    inbound esp sas:
     spi: 0xD3E9ABD0(3555306448)
       transform: esp-3des ,
       in use settings ={Tunnel, }
       conn id: 2006, flow_id: 6, crypto map: to-peer-outside
       sa timing: remaining key lifetime (k/sec): (4586265/3542)
            HA last key lifetime sent(k): (4586267)
       ike_cookies: 9263635C CA4B4E99 C14E908E 8EE2D79C
       IV size: 8 bytes
       replay detection support: Y
       Status: ACTIVE
```

Table 100 describes the significant fields shown in the preceding **show crypto ipsec sa active** display. Additional fields are self-explanatory or can be found in Table 98 or Table 99.

Table 100 show crypto ipsec sa active Field Descriptions.

Field	Description
HA last key lifetime sent (k)	Last stored kilobytes lifetime value for HA.
ike_cookies	ID that identifies the IKE SAs.

The following sample output shows the IPsec SA status of only the standby device. The fields in the display are either self-explanatory or can be found in Table 98, Table 99, or Table 100.

```
Router# show crypto ipsec sa standby

interface: Ethernet0/0
    Crypto map tag: to-peer-outside, local addr 10.165.201.3

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.0.1/255.255.255.255/0/0)
   remote ident (addr/mask/prot/port): (172.16.0.1/255.255.255.255/0/0)
   current_peer 209.165.200.225 port 500
     PERMIT, flags={origin_is_acl,}
    #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.: 209.165.201.3, remote crypto endpt.: 209.165.200.225
     path mtu 1500, media mtu 1500
     current outbound spi: 0xD42904F0(3559458032)

     inbound esp sas:
      spi: 0xD3E9ABD0(3555306448)
        transform: esp-3des ,
        in use settings ={Tunnel, }
        conn id: 2012, flow_id: 12, crypto map: to-peer-outside
        sa timing: remaining key lifetime (k/sec): (4441561/3486)
             HA last key lifetime sent(k): (4441561)
        ike_cookies: 00000000 00000000 00000000 00000000
        IV size: 8 bytes
        replay detection support: Y
        Status: STANDBY

     inbound ah sas:
```

```
 spi: 0xF3EE3620(4092474912)
   transform: ah-md5-hmac ,
   in use settings ={Tunnel, }
   conn id: 2012, flow_id: 12, crypto map: to-peer-outside
   sa timing: remaining key lifetime (k/sec): (4441561/3486)
        HA last key lifetime sent(k): (4441561)
   ike_cookies: 00000000 00000000 00000000 00000000
   replay detection support: Y
   Status: STANDBY

inbound pcp sas:

outbound esp sas:
 spi: 0xD42904F0(3559458032)
   transform: esp-3des ,
   in use settings ={Tunnel, }
   conn id: 2011, flow_id: 11, crypto map: to-peer-outside
   sa timing: remaining key lifetime (k/sec): (4441561/3485)
        HA last key lifetime sent(k): (4441561)
   ike_cookies: 00000000 00000000 00000000 00000000
   IV size: 8 bytes
   replay detection support: Y
   Status: STANDBY

outbound ah sas:
 spi: 0x75251086(1965363334)
   transform: ah-md5-hmac ,
   in use settings ={Tunnel, }
   conn id: 2011, flow_id: 11, crypto map: to-peer-outside
   sa timing: remaining key lifetime (k/sec): (4441561/3485)
        HA last key lifetime sent(k): (4441561)
   ike_cookies: 00000000 00000000 00000000 00000000
   replay detection support: Y
   Status: STANDBY

outbound pcp sas:
```

Related Commands

Command	Description
crypto ipsec security-association	Configures the IPSec security associations.

show crypto ipsec security-association idle-time

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

show crypto ipsec security-association idle-time

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SRB	This command was introduced in a release earlier than Cisco IOS Release 12.2(33)SRB.
12.2SX	This command was integrated into Cisco IOS Release 12.2SX.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
Cisco IOS XE 2.3	This command was integrated into Cisco IOS XE Release 2.3.

Usage Guidelines

Use the **show crypto ipsec security-association idle-time** command to display the idle time.

When a router running the Cisco IOS software creates an IPsec SA for a peer, resources must be allocated to maintain the SA. The SA requires both memory and several managed timers. For idle peers, these resources are wasted. If enough resources are wasted by idle peers, the router could be prevented from creating new SAs with other peers. The IPsec Security Association Idle Timers feature introduces a configurable idle timer to monitor SAs for activity, allowing SAs for idle peers to be deleted. This increases the availability of the resources and improve scalability of Cisco IOS IPsec deployments.

Examples

The following is a sample output from the **show crypto ipsec security-association idle-time** command. The output is self-explanatory.

```
Router# show crypto ipsec security-association idle-time

Security association idletime: 567 seconds
```

Related Commands

Command	Description
show crypto ipsec security-association lifetime	Displays the SA lifetime value configured for a particular crypto map entry.

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 privileged EXEC mode.

show crypto ipsec security-association lifetime

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.3 T	This command was introduced.\
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

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 or active default transform sets, use the **show crypto ipsec transform-set** command in privileged EXEC mode.

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

Syntax Description

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

Command Modes

Privileged 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.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(20)T	The command output was expanded to include information about active default transform sets.
Cisco IOS XE Release 2.4	This command was implemented on the Cisco ASR 1000 series routers.

Usage Guidelines

There are two default transform sets supported in Cisco IOS k9 images only:

- Esp-aes esp-sha-hmac
- Esp-3des esp-sha-hmac

The **show crypto ipsec transform-set** command will display the default transform sets if there are no other transform set configured, you have not disabled the default transform sets by issuing the **no crypto ipsec default transform-set** command, and the crypto engine supports the encryption algorithm.

Examples

The following is sample output for the **show crypto ipsec transform-set** command when the default transform sets have been disabled with the **no crypto ipsec default 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
no crypto ipsec default transform-set
```

The following sample output from the s**how 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
```

The following is sample output for the **show crypto ipsec transform-set** command when the default transform sets are active and the crypto engine supports the encryption algorithm:

```
Router# show crypto ipsec transform-set

Transform set asset: { esp-256-aes esp-sha-hmac  }
   will negotiate = { Transport,  },

Transform set aesset: { esp-256-aes esp-sha-hmac  }
   will negotiate = { Transport,  },

Transform set #$!default_transform_set_1: { esp-aes esp-sha-hmac  }
   will negotiate = { Transport,  },

Transform set #$!default_transform_set_0: { esp-3des esp-sha-hmac  }
   will negotiate = { Transport,  },
```

Related Commands

Command	Description
show crypto ipsec default transform-set	Displays the default IPsec transform sets.
show crypto ipsec transform-set	Displays the configured transform sets.
show crypto map (IPsec)	Displays the crypto map configuration.

show crypto isakmp default policy

To display the default Internet Key Exchange (IKE) policies currently in use, use the **show crypto isakmp default policy** command in privileged EXEC mode.

show crypto isakmp default policy

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(20)T	This command was introduced.
Cisco IOS XE Release 2.4	This command was implemented on the Cisco ASR 1000 series routers.

Usage Guidelines

If you have neither manually configured IKE policies with the **crypto isakmp policy** command nor issued the **no crypto isakmp default policy** command, IPsec will use the default IKE policies to negotiate IKE proposals. There are eight default IKE default policies supported (see Table 101). The default IKE policies define the following policy set parameters:

- The priority, 65507–65514, where 65507 is the highest priority and 65514 is the lowest priority.
- The authentication method, Rivest, Shamir, and Adelman (RSA) or preshared keys (PSK).
- The encryption method, Advanced Encryption Standard (AES) or Triple Data Encryption Standard (3DES).
- The hash function, Secure Hash Algorithm (SHA-1) or Message-Digest algorithm 5 (MD5).
- The Diffie-Hellman (DH) group specification DH2 or DH5.
  - DH2 specifies the 768-bit Diffie-Hellman group.
  - DH5 specifies the 1536-bit Diffie-Hellman group.

Table 101 Default IKE Policies

Priority	Authentication	Encryption	Hash	Diffie-Hellman
65507	RSA	AES	SHA	DH5
65508	PSK	AES	SHA	DH5
65509	RSA	AES	MD5	DH5
65510	PSK	AES	MD5	DH5
65511	RSA	3DES	SHA	DH2
65512	PSK	3DES	SHA	DH2
65513	RSA	3DES	MD5	DH2
65514	PSK	3DES	MD5	DH2

If you have manually configured IKE policies and you issue the **show crypto isakmp default policy** command there is no output, since the default IKE policies are not in use.

Examples

The following example displays the eight default policies with protection suites of priorities 65507–65014. The default policies are displayed since there are no user configured policies, the default policies have not been disabled, and EzVPN is not configured.

```
Router# show crypto isakmp default policy

Default protection suite of priority 65507
        encryption algorithm:   AES - Advanced Encryption Standard (128 bit keys).
        hash algorithm:         Secure Hash Standard
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #5 (1536 bit)
        lifetime:               86400 seconds, no volume limit
Default protection suite of priority 65508
        encryption algorithm:   AES - Advanced Encryption Standard (128 bit keys).
        hash algorithm:         Secure Hash Standard
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #5 (1536 bit)
        lifetime:               86400 seconds, no volume limit
Default protection suite of priority 65509
        encryption algorithm:   AES - Advanced Encryption Standard (128 bit keys).
        hash algorithm:         Message Digest 5
        authentication method:  Rivest-Shamir-Adleman signature
        Diffie-Hellman group:   #5 (1536 bit)
        lifetime:               86400 seconds, no volume limit
Default protection suite of priority 65510
        encryption algorithm:   AES - Advanced Encryption Standard (128 bit keys).
        hash algorithm:         Message Digest 5
        authentication method:  pre-shared key
        Diffie-Hellman group:   #5 (1536 bit)
        lifetime:               86400 seconds, no volume limit
Default protection suite of priority 65511
        encryption algorithm:   Three key triple DES
        hash algorithm:         Secure Hash Standard
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               86400 seconds, no volume limit
Default protection suite of priority 65512
        encryption algorithm:   Three key triple DES
        hash algorithm:         Secure Hash Standard
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               86400 seconds, no volume limit
Default protection suite of priority 65513
        encryption algorithm:   Three key triple DES
        hash algorithm:         Message Digest 5
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               86400 seconds, no volume limit
Default protection suite of priority 65514
        encryption algorithm:   Three key triple DES
        hash algorithm:         Message Digest 5
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               86400 seconds, no volume limit
```

The following example shows that there is no output from the **show crypto isakmp default policy** command when the default policies have been disabled.

```
Router(config)# no crypto isakmp default policy
! The default IKE policies have been disabled.
Router(config)# exit
Router# configure terminal
Router# show crypto isakmp default policy
Router#
! There is no output from the show crypto isakmp default policy command.
```

Related Commands

Command	Description
crypto isakmp policy	Defines an IKE policy.
no crypto isakmp default policy	Disables IKE default policies.
show crypto isakmp policy	Displays the parameters for each IKE policy.

show crypto isakmp key

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

show crypto isakmp key

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.4(4)T	IPv6 address information was added to command output.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

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 102 describes significant fields in the **show crypto isakmp key** profile.

Table 102 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 Private Network routing and forwarding (VRF) of the keyring. If the keyring does not have a VRF, an empty string is printed.

show crypto isakmp peers

To display the Internet Security Association and Key Management Protocol (ISAKMP) peer descriptions, use the **show crypto isakmp peers** command in privileged EXEC mode.

show crypto isakmp peers [*ipaddress* | *ipv6address* | **config** [*peername*]]

Syntax Description

ipaddress	(Optional) The IP address of the specific peer. **Note** If the optional *ipaddress* argument is not included with the command, a summarization of all peers is displayed.
ipv6address	(Optional) The IPv6 address of the specific peer.
config	(Optional) Displays detailed information about all peers or a specific peer.
peername	(Optional) The peer name.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
12.4(4)T	The **config** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.(33)SRA.
12.4(11)T	The **show crypto isakmp peer** command name was changed to **show crypto isakmp peers**.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1 on the Cisco ASR 1000 Series Routers.

Usage Guidelines

Before you can use the **config** keyword, the following commands must be enabled for the accounting update to work correctly: **aaa accounting update** with **new info** keyword and **radius-server vsa send** with **accounting** keyword.

Examples

The following output example shows information about the peer named "This-is-another-peer-at-10-1-1-3":

```
Router# show crypto isakmp peers

Peer: 10.1.1.3 Port: 500
 Description: This-is-another-peer-at-10-1-1-3
 Phase1 id: 10.1.1.3
```

In the following example, the **config** keyword is used to display all manageability information for an Easy VPN remote device. Cisco Easy VPN is an IP Security (IPsec) virtual private network (VPN) solution supported by Cisco routers and security appliances. It greatly simplifies VPN deployment for remote offices and mobile workers. The fields are self-explanatory.

```
Router# show crypto isakmp peers config

Client-Public-Addr=192.168.10.2:500; Client-Assigned-Addr=172.16.1.209;
Client-Group=branch; Client-User=branch; Client-Hostname=branch.; Client-Platform=Cisco
1711; Client-Serial=FOC080210E2 (412454448); Client-Config-Version=11;
Client-Flash=33292284; Client-Available-Flash=10202680; Client-Memory=95969280;
Client-Free-Memory=14992140; Client-Image=flash:c1700-advipservicesk9-mz.ef90241;

Client-Public-Addr=192.168.10.3:500; Client-Assigned-Addr=172.16.1.121;
Client-Group=store; Client-User=store; Client-Hostname=831-storerouter.;
Client-Platform=Cisco C831; Client-Serial=FOC08472UXR (1908379618);
Client-Config-Version=2; Client-Flash=24903676; Client-Available-Flash=5875028;
Client-Memory=45298688; Client-Free-Memory=6295596;
Client-Image=flash:c831-k9o3y6-mz.ef90241
```

Related Commands

Command	Description
aaa accounting update	Enables the periodic interim accounting records to be sent to the accounting server.
radius-server vsa send	Configures the network access server (NAS) to recognize and use vendor-specific attributes (VSAs).
clear crypto session	Deletes crypto sessions (IPSec and IKE) SAs.
show crypto session	Displays status information for active crypto sessions in a router.

show crypto isakmp policy

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

show crypto isakmp policy

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.3T	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.
12.4(4)T	Support for IPv6 was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(20)T	The command output was expanded to include default IKE policies.
Cisco IOS XE Release 2.4	This command was implemented on the Cisco ASR 1000 series routers.

Usage Guidelines

There are eight default IKE default policies supported with protection suites of priorities 65507–65514, where 65507 is the highest priority and 65514 is the lowest priority. If you have neither manually configured IKE policies with the **crypto isakmp policy** command nor disabled the default IKE policies by issuing the **no crypto isakmp default policy** command, the default IKE policies will be displayed when the **show crypto isakmp policy** command is issued.

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
```

The following sample output from the **show crypto isakmp policy** command displays the default IKE policies. The manually configured IKE policies with priorities 10 and 20 have been removed.

```
Router(config)# no crypto isakmp policy 10
Router(config)# no crypto isakmp policy 20
Router(config)# exit
R1# show crypto isakmp policy

Default IKE policy
Protection suite of priority 65507
        encryption algorithm:   AES - Advanced Encryption Standard (128 bit key.
        hash algorithm:         Secure Hash Standard
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #5 (1536 bit)
        lifetime:               86400 seconds, no volume limit
Protection suite of priority 65508
        encryption algorithm:   AES - Advanced Encryption Standard (128 bit key.
        hash algorithm:         Secure Hash Standard
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #5 (1536 bit)
        lifetime:               86400 seconds, no volume limit
Protection suite of priority 65509
        encryption algorithm:   AES - Advanced Encryption Standard (128 bit key.
        hash algorithm:         Message Digest 5
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #5 (1536 bit)
        lifetime:               86400 seconds, no volume limit
Protection suite of priority 65510
        encryption algorithm:   AES - Advanced Encryption Standard (128 bit key.
        hash algorithm:         Message Digest 5
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #5 (1536 bit)
        lifetime:               86400 seconds, no volume limit
Protection suite of priority 65511
        encryption algorithm:   Three key triple DES
        hash algorithm:         Secure Hash Standard
```

```
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               86400 seconds, no volume limit
Protection suite of priority 65512
        encryption algorithm:   Three key triple DES
        hash algorithm:         Secure Hash Standard
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               86400 seconds, no volume limit
Protection suite of priority 65513
        encryption algorithm:   Three key triple DES
        hash algorithm:         Message Digest 5
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               86400 seconds, no volume limit
Protection suite of priority 65514
        encryption algorithm:   Three key triple DES
        hash algorithm:         Message Digest 5
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               86400 seconds, no volume limit
```

The field descriptions in the display are self-explanatory.

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 default policy	Displays the default IKE policies.

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 privileged EXEC mode.

show crypto isakmp profile [**tag** *profilename* | **vrf** *vrfname*]

Syntax Description

tag *profilename*	(Optional) Displays ISAKMP profile details specified by the profile name.
vrf *vrfname*	(Optional) Displays ISAKMP profile details specified by the VPN routing/forwarding instance (VRF) name.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.4(4)T	IPv6 support was added.
12.4(11)T	The **tag** *profilename* and **vrf** *vrfname* keywords and arguments were added.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Examples

The following is sample output from 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
```

The following sample output shows information for an IPv6 router:

```
Router# show crypto isakmp profile

ISAKMP PROFILE tom
Identities matched are:
ipv6-address 2001:0DB8:0:1::1/32
Certificate maps matched are:
Identity presented is: ipv6-address fqdn
keyring(s): <none>
trustpoint(s): <all>
```

Table 103 describes the significant fields shown in the display.

Table 103 show crypto isakmp profile Field Descriptions

Field	Description
ISAKMP PROFILE	Name of the ISAKMP profile.

Table 103 show crypto isakmp profile Field Descriptions

Field	Description
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 preceding **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 current Internet Key Exchange (IKE) security associations (SAs), use the **show crypto isakmp sa** command in privileged EXEC mode.

show crypto isakmp sa [**active** | **standby** | **detail** | **nat**] [**vrf** *vrfname*]

Syntax Description

active	(Optional) Displays high availability- (HA-) enabled Internet Security Association and Key Management Protocol (ISAKMP) SAs that are in the active state.
standby	(Optional) Displays HA-enabled ISAKMP SAs that are in the standby state.
detail	(Optional) Displays all existing IKE SAs, whether in an active or standby state.
nat	(Optional) Displays IKE SAs that have undergone network address translation (NAT).
vrf *vrfname*	(Optional) Displays IKE SA details about the specified VRF. • The *vrfname* value is the name of the VRF.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.3 T	This command was introduced.
12.3(11)T	The **active** and **standby** keywords were added.
12.4(4)T	IPv6 information was added to the command output. The **detail** and **nat** keywords were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.(33)SRA.
12.4(11)T	The **vrf** *vrfname* keyword and argument were added.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If neither the **active** keyword nor the **standby** keyword is specified, current SAs for all configured routers will be shown. Use the **nat** keyword to display the IP address and port address of a remote peer when NAT is used.

Examples

The following sample output shows the SAs of both the active and standby devices:

```
Router# show crypto isakmp sa

dst             src             state          conn-id slot status
10.165.201.3   10.165.200.225 QM_IDLE              2    0 STDBY
10.0.0.1        10.0.0.2        QM_IDLE             1    0 ACTIVE
```

The following sample output shows the SAs of only the active device:

```
Router# show crypto isakmp sa active

dst             src             state          conn-id slot status
10.165.201.3    10.165.200.225 QM_IDLE             5    0 ACTIVE
```

The following sample output shows the SAs of only the standby device:

```
Router# show crypto isakmp sa standby

dst             src             state          conn-id slot status
10.165.201.3    10.165.200.225 QM_IDLE             5    0 STDBY
10.165.201.3    10.165.200.225 QM_IDLE             1    0 STDBY
```

The following sample output shows the SAs of an active IPv6 device. The IPv4 device is inactive.

```
Router# show crypto isakmp sa detail

Codes: C - IKE configuration mode, D - Dead Peer Detection
       K - Keepalives, N - NAT-traversal
       X - IKE Extended Authentication
       psk - Preshared key, rsig - RSA signature
       renc - RSA encryption
IPv4 Crypto ISAKMP SA

C-id  Local           Remote          I-VRF    Status Encr Hash Auth DH
Lifetime Cap.

IPv6 Crypto ISAKMP SA

  dst: 3FFE:2002::A8BB:CCFF:FE01:2C02
  src: 3FFE:2002::A8BB:CCFF:FE01:9002
  conn-id: 1001  I-VRF:          Status: ACTIVE Encr: des  Hash: sha  Auth:
psk
  DH: 1  Lifetime: 23:45:00 Cap: D    Engine-id:Conn-id = SW:1

  dst: 3FFE:2002::A8BB:CCFF:FE01:2C02
  src: 3FFE:2002::A8BB:CCFF:FE01:9002
  conn-id: 1002  I-VRF:          Status: ACTIVE Encr: des  Hash: sha  Auth:
psk
  DH: 1  Lifetime: 23:45:01 Cap: D    Engine-id:Conn-id = SW:2
```

Table 104 through Table 107 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 main mode (MM_xxx) states may be observed.

Table 104 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.

Table 104 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_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 105 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 106 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 107 show crypto isakmp sa Field Descriptions

Field	Description
f_vrf/i_vrf (not shown)	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.

show crypto key mypubkey rsa

To display the RSA public keys of your router, use the **show crypto key mypubkey rsa** command in privileged EXEC mode.

show crypto key mypubkey rsa

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.3 T	This command was introduced.
12.3(7)T	The show output was modified to display whether an RSA key is protected (encrypted) and locked or unlocked.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
15.0(1)M	This command was modified to display whether redundancy is specified in the **crypto_key_generate_rsa command**.

Usage Guidelines

This command displays the RSA public keys of your router.

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

Examples

The following is sample output from the **show crypto key mypubkey rsa** command. Special usage RSA keys were previously generated for this router using the **crypto key generate rsa** command.

```
% Key pair was generated at: 06:07:49 UTC Jan 13 1996
Key name: myrouter.example.com
 Usage: Signature Key
 Key Data:
  005C300D 06092A86 4886F70D 01010105 00034B00 30480241 00C5E23B 55D6AB22
  04AEF1BA A54028A6 9ACC01C5 129D99E4 64CAB820 847EDAD9 DF0B4E4C 73A05DD2
  BD62A8A9 FA603DD2 E2A8A6F8 98F76E28 D58AD221 B583D7A4 71020301 0001

% Key pair was generated at: 06:07:50 UTC Jan 13 1996
Key name: myrouter.example.com
 Usage: Encryption Key
 Key Data:
  00302017 4A7D385B 1234EF29 335FC973 2DD50A37 C4F4B0FD 9DADE748 429618D5
  18242BA3 2EDFBDD3 4296142A DDF7D3D8 08407685 2F2190A0 0B43F1BD 9A8A26DB
  07953829 791FCDE9 A98420F0 6A82045B 90288A26 DBC64468 7789F76E EE21
```

The following example shows how to encrypt the RSA key "pki1-72a.cisco.com." Thereafter, the **show crypto key mypubkey rsa** command is issued to verify that the RSA key is encrypted (protected) and unlocked.

```
Router(config)# crypto key encrypt rsa name pki1-72a.cisco.com passphrase cisco1234
Router(config)# exit
Router# show crypto key mypubkey rsa

% Key pair was generated at:00:15:32 GMT Jun 25 2003
Key name:pki1-72a.cisco.com
Usage:General Purpose Key
*** The key is protected and UNLOCKED. ***
Key is not exportable.
Key Data:
305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00E0CC9A 1D23B52C
CD00910C ABD392AE BA6D0E3F FC47A0EF 8AFEE340 0EC1E62B D40E7DCC
23C4D09E
03018B98 E0C07B42 3CFD1A32 2A3A13C0 1FF919C5 8DE9565F 1F020301 0001
% Key pair was generated at:00:15:33 GMT Jun 25 2003
Key name:pki1-72a.cisco.com.server
Usage:Encryption Key
Key is exportable.
Key Data:
307C300D 06092A86 4886F70D 01010105 00036B00 30680261 00D3491E 2A21D383
854D7DA8 58AFBDAC 4E11A7DD E6C40AC6 66473A9F 0C845120 7C0C6EC8 1FFF5757
3A41CE04 FDCB40A4 B9C68B4F BC7D624B 470339A3 DE739D3E F7DDB549 91CD4DA4
DF190D26 7033958C 8A61787B D40D28B8 29BCD0ED 4E6275C0 6D020301 0001
Router#
```

The following example shows how to lock the key "pki1-72a.cisco.com." Thereafter, the **show crypto key mypubkey rsa** command is issued to verify that the key is protected (encrypted) and locked.

```
Router# crypto key lock rsa name pki1-72a.cisco.com passphrase cisco1234
!
Router# show crypto key mypubkey rsa

% Key pair was generated at:20:29:41 GMT Jun 20 2003
Key name:pki1-72a.cisco.com
Usage:General Purpose Key
*** The key is protected and LOCKED. ***
Key is exportable.
Key Data:
305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00D7808D C5FF14AC
0D2B55AC 5D199F2F 7CB4B355 C555E07B 6D0DECBE 4519B1F0 75B12D6F 902D6E9F
B6FDAD8D 654EF851 5701D5D7 EDA047ED 9A2A619D 5639DF18 EB020301 0001
```

The string "Redundancy enabled" in the following example indicates that the **redundancy** keyword was specified when the key was generated by the **crypto_key_generate_rsa command**.

```
Router#show crypto key mypubkey rsa MYKEYS
% Key pair was generated at: 07:38:04 GMT Oct 02 2009
Key name: MYKEYS
 Storage Device: not specified
 Usage: General Purpose Key
 Key is not exportable. Redundancy enabled.
 Key Data:
  305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00A63726 28C9EE7D
  A89AF6E1 5B42A854 A76EDF9F 35681024 A7868113 B93E2384 EF15CD78 8467A797
  F946268F 067FF15E A1734BE6 3E3444C2 BAE00618 BCAED5A3 BB020301 0001
```

Related Commands

Command	Description
crypto key encrypt rsa	Encrypts the RSA private key.
crypto key generate rsa	Generates RSA key pairs.
crypto key lock rsa	Locks the RSA private key in a router.

show crypto key pubkey-chain rsa

To display the RSA public keys of the peer that are stored on the router, use the **show crypto key pubkey-chain rsa** command in user EXEC mode or privileged EXEC mode.

show crypto key pubkey-chain rsa [**address** *key-address* | **name** *key-name* | **vrf** *vrf-name* [**address** *ip-address*]]

Syntax Description

address *key-address*	(Optional) Address of a specific key to view.
name *key-name*	(Optional) Name of a specific key to view.
vrf *vrf-name*	(Optional) Name of a specific Virtual Private Network (VPN) Routing and Forwarding (VRF) instance for which to display keys.
address *ip-address*	(Optional) IP address belonging to a VRF instance.

Command Default

Information is displayed for all RSA public keys stored on the router.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
11.3T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

The keys that are displayed include peers' RSA public keys that are manually configured at the router and keys that are received by the router via other means (such as by a certificate, if certification authority support is configured).

If a router reboots, any keys derived by certificates are lost. This is because the router requests certificates again (then the keys are derived again).

Examples

The following example shows how to display information for all RSA public keys stored on the router:

```
Router# show crypto key pubkey-chain rsa

Codes: M - Manually Configured, C - Extracted from certificate

Code Usage         IP-address            Keyring          Name
M    Signature     209.165.200.225       default          myrouter.example.com
M    Encryption    209.165.202.129       default          myrouter.example.com
```

```
C     Signature    209.165.200.225        default          routerA.example.com
C     Encryption   209.165.202.129        default          routerA.example.com
C     General      209.165.200.225        default          routerB.domain1.com
```

The example above shows manually configured special usage RSA public keys for the peer myrouter.example.com. This sample also indicates certificate support and therefore shows three keys obtained from peers' certificates: special usage keys for peer routerA.example.com and a general purpose key for peer routerB.domain1.com.

The following example shows how to display keys for a specific VRF instance.

```
Router# show crypto key pubkey-chain rsa vrf
Code Usage         IP-Address/VRF         Keyring          Name
M    General       209.165.200.225        default          Key_1
M    General       209.165.202.129        default          Key_2
```

The following example shows how to display details for a key named somerouter.example.com:

```
Router# show crypto key pubkey-chain rsa name somerouter.example.com

Key name: somerouter.example.com
Key address: 209.165.200.225
 Usage: Signature Key
 Source: Manual
 Data:
  305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00C5E23B 55D6AB22
  04AEF1BA A54028A6 9ACC01C5 129D99E4 64CAB820 847EDAD9 DF0B4E4C 73A05DD2
  BD62A8A9 FA603DD2 E2A8A6F8 98F76E28 D58AD221 B583D7A4 71020301 0001

Key name: somerouter.example.com
Key address: 209.165.200.225
 Usage: Encryption Key
 Source: Manual
 Data:
  00302017 4A7D385B 1234EF29 335FC973 2DD50A37 C4F4B0FD 9DADE748 429618D5
  18242BA3 2EDFBDD3 4296142A DDF7D3D8 08407685 2F2190A0 0B43F1BD 9A8A26DB
  07953829 791FCDE9 A98420F0 6A82045B 90288A26 DBC64468 7789F76E EE21
```

Note The Source field in the above example displays "Manual," which means that the keys were manually configured on the router (and not received in the peer's certificate).

The following example shows how to display details for a key with address 209.165.202.129:

```
Router# show crypto key pubkey-chain rsa address 209.165.202.129

Key name: routerB.example.com
Key address: 209.165.202.129
 Usage: General Purpose Key
 Source: Certificate
 Data:
  0738BC7A 2BC3E9F0 679B00FE 53987BCC 01030201 42DD06AF E228D24C 458AD228
  58BB5DDD F4836401 2A2D7163 219F882E 64CE69D4 B583748A 241BED0F 6E7F2F16
  0DE0986E DF02031F 4B0B0912 F68200C4 C625C389 0BFF3321 A2598935 C1B1
```

Note The Source field in the above example displays "Certificate," which means that the keys were received by the router from the certificate authority.

Table 108 describes the significant fields shown in the displays.

Table 108 show crypto key pubkey-chain rsa Field Descriptions

Field	Description
Code	Source of the key: M (manually configured at the router) or C (received by the router via a certificate).
Usage	Purpose of the key: general purpose, signature, or encryption).
IP-Address/VRF	IP address or VRF of the key.
Keyring	Name of the keyring that stores the key. The possible values are either the name of a user-defined keyring or default (the default keyring).
Name	Name of the key. For manually inserted keys (code M), this name is manually configured. For keys that are extracted from the certificate (code C) the name is the subject name in the certificate itself.
Data	The contents of the key itself.

Related Commands

Command	Description
crypto key pubkey-chain rsa	Enters public key configuration mode (so you can manually specify other devices' RSA public keys).
rsa-pubkey	Defines the RSA manual key to be used for encryption or signature during IKE authentication.

show crypto map (IPsec)

To display the crypto map configuration, use the **show crypto map** command in user EXEC or privileged EXEC mode.

show crypto map [**gdoi fail-close** *map-name* | **interface** *interface* | **tag** *map-name*]

Syntax Description

gdoi	(Optional) Displays information about the status of the Group Domain of Interpretation (GDOI) fail-close mode.
fail-close	Specifies the list of crypto maps configured with the fail-close mode.
map-name	Name of the specified crypto map.
interface *interface*	(Optional) Displays only the crypto map set that is applied to the specified interface.
tag	(Optional) Displays only the crypto map set that is specified.

Command Default

No crypto maps are displayed.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
11.2	This command was introduced.
12.3(8)T	This command was integrated into Cisco IOS Release 12.3(8)T. The output was modified to display the crypto input and output Access Control Lists (ACLs) that have been configured.
12.4(4)T	This command was integrated into Cisco IOS Release 12.4(4)T. IPv6 address information was added to command output.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.(33)SRA.
12.2SX	This command was integrated into Cisco IOS Release 12.2SX. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T. The default transform set information was added to command output.
12.4(22)T	This command was integrated into Cisco IOS Release 12.4(22)T. The **gdoi fail-close** keywords and the *map-tag* arguments were added.
Cisco IOS XE Release 2.3	This command was modified. It was integrated into Cisco IOS XE Release 2.3.

Usage Guidelines

The **show crypto map** command allows you to specify a particular crypto map. The crypto maps shown in the command output are dynamically generated; you need not configure crypto maps in order for them to appear in this command output.

Two default transform sets are supported in Cisco IOS K9 images only:

- Esp-aes esp-sha-hmac
- Esp-3des esp-sha-hmac

The **show crypto map** command displays the default transform sets if no other transform sets are configured for the crypto map, if you have not disabled the default transform sets by issuing the **no crypto ipsec default transform-set** command, and if the crypto engine supports the encryption algorithm.

Examples

The following example shows that crypto input and output ACLs have been configured:

```
Router# show crypto map

Crypto Map "test" 10 ipsec-isakmp
 Peer
 Extended IP access list ipsec_acl
  access-list ipsec_acl permit ip 192.168.2.0 0.0.0.255 192.168.102.0 0.0.0.255
 Extended IP access check IN list 110
  access-list 110 permit ip host 192.168.102.47 192.168.2.0 10.0.0.15
  access-list 110 permit ip host 192.168.102.47 192.168.2.32 10.0.0.15
  access-list 110 permit ip host 192.168.102.47 192.168.2.64 10.0.0.15
  access-list 110 permit ip host 192.168.102.57 192.168.2.0 10.0.0.15
  access-list 110 permit ip host 192.168.102.57 192.168.2.32 10.0.0.15
  access-list 110 permit ip host 192.168.102.57 192.168.2.64 10.0.0.15
 Extended IP access check OUT list 120
  access-list 120 permit ip 192.168.2.0 10.0.0.15 host 192.168.102.47
  access-list 120 permit ip 192.168.2.32 10.0.0.15 host 192.168.102.47
  access-list 120 permit ip 192.168.2.64 10.0.0.15 host 192.168.102.47
  access-list 120 permit ip 192.168.2.0 10.0.0.15 host 192.168.102.57
  access-list 120 permit ip 192.168.2.32 10.0.0.15 host 192.168.102.57
  access-list 120 permit ip 192.168.2.64 10.0.0.15 host 192.168.102.57
 Current peer: 10.0.0.2
 Security association lifetime: 4608000 kilobytes/3600 seconds
 PFS (Y/N): N
 Transform sets=test
 Interfaces using crypto map test:
  Serial0/1
```

Table 109 describes the significant fields shown in the display.

Table 109 show crypto map Field Descriptions

Field	Description
Peer	Possible peers that are configured for this crypto map entry.
Extended IP access list	Access list that is used to define the data packets that need to be encrypted. Packets that are denied by this access list are forwarded but not encrypted. The “reverse” of this access list is used to check the inbound return packets, which are also encrypted. Packets that are denied by the “reverse” access list are dropped because they should have been encrypted but were not.

Table 109 show crypto map Field Descriptions (continued)

Field	Description
Extended IP access check	Access lists that are used to more finely control which data packets are allowed into or out of the IPsec tunnel. Packets that are allowed by the "Extended IP access list" ACL but denied by the "Extended IP access list check" ACL are dropped.
Current peer	Current peer that is being used for this crypto map entry.
Security association lifetime	Number of bytes that are allowed to be encrypted or decrypted or the age of the security association before new encryption keys must be negotiated.
PFS	(Perfect Forward Secrecy) If the field is marked as 'Yes', the Internet Security Association and Key Management Protocol (ISAKMP) SKEYID-d key is renegotiated each time security association (SA) encryption keys are renegotiated (requires another Diffie-Hillman calculation). If the field is marked as 'No', the same ISAKMP SKEYID-d key is used when renegotiating SA encryption keys. ISAKMP keys are renegotiated on a separate schedule, with a default time of 24 hours.
Transform sets	List of transform sets (encryption, authentication, and compression algorithms) that can be used with this crypto map.
Interfaces using crypto map test	Interfaces to which this crypto map is applied. Packets that are leaving from this interface are subject to the rules of this crypto map for encryption. Encrypted packets may enter the router on any interface, and they are decrypted. Nonencrypted packets that are entering the router through this interface are subject to the "reverse" crypto access list check.

The following example displays output from the **show crypto map** command. No transform sets are configured for the crypto map "mymap," the default transform sets are enabled, and the crypto engine supports the encryption algorithm.

```
Router# show crypto map

Crypto Map "mymap" 1 ipsec-isakmp
        Peer = 209.165.201.1
        Extended IP access list 102
            access-list 102 permit ip 192.168.1.0 0.0.0.255 10.0.0.0 0.0.255.255
        Security association lifetime: 4608000 kilobytes/3600 seconds
        PFS (Y/N): N
        Transform sets={
                #$!default_transform_set_1:  { esp-aes esp-sha-hmac  } ,
                #$!default_transform_set_0:  { esp-3des esp-sha-hmac  } ,
        }
        Reverse Route Injection Enabled
        Interfaces using crypto map mymap:
```

The following example displays output of the **show crypto map** command. No transform sets configured for the crypto map "mymap" and the default transform sets have been disabled.

```
Router(config)# no crypto ipsec default transform-set
Router(config)# exit
Router# configure terminal
Router# show crypto map

Crypto Map "mymap" 1 ipsec-isakmp
        Peer = 209.165.201.1
        Extended IP access list 102
            access-list 102 permit ip 192.168.1.0 0.0.0.255 10.0.0.0 0.0.255.255
        Security association lifetime: 4608000 kilobytes/3600 seconds
        PFS (Y/N): N
        Transform sets={
        }


! There are no transform sets for the crypto map "mymap."
        Reverse Route Injection Enabled
        Interfaces using crypto map mymap:
```

The following example displays output for the **show crypto map** command and **gdoi fail-close** keywords (**show crypto map gdoi fail-close**). Fail-close has been activated. In addition, an implicit "permit ip any any" entry is configured, causing any traffic other than Telnet and Open Shortest Path First (OSPF) to be dropped:

```
Router# show crypto map gdoi fail-close 23

Crypto Map: "svn"
        Activate: yes
        Fail-Close Access-List: (Deny = Forward In Clear, Permit = Drop)
            access-list 105 deny tcp any port = 23 any
            access-list 105 deny ospf any any
```

Related Commands

Command	Description
show crypto ipsec default transform-set	Displays the default IPsec transform sets.
show crypto ipsec transform-set	Displays the configured transform sets.

show crypto mib ipsec flowmib endpoint

To display the IP Security (IPsec) phase-2 tunnel endpoint table, use the **show crypto mib ipsec flowmib endpoint** command in privileged EXEC mode.

show crypto mib ipsec flowmib endpoint [**vrf** *vrf-name*]

Syntax Description

vrf *vrf-name*	(Optional) Displays the parameters for the specified Virtual Private Network (VPN) routing and forwarding (VRF) instance.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(20)T	This command was introduced.
Cisco IOS XE Release 2.4	This command was implemented on the Cisco ASR 1000 series routers.

Usage Guidelines

The IPsec phase-2 tunnel endpoint table contains an entry for each active endpoint associated with an IPsec phase-2 tunnel.

Examples

The following example displays the IPsec phase 2 tunnel endpoint table for all VRFs:

```
Router# show crypto mib ipsec flowmib endpoint

vrf Global
  Index:               1
  Local type:          Single IP address
  Local address:       192.1.2.1
  Protocol:            0
  Local port:          0
  Remote type:         Single IP address
  Remote address:      192.1.2.2
  Remote port:         0

  Index:               2
  Local type:          Subnet
  Local address:       192.1.3.0 255.255.255.0
  Protocol:            0
  Local port:          0
  Remote type:         Subnet
  Remote address:      192.1.3.0 255.255.255.0
  Remote port:         0
```

Table 110 describes the significant fields shown in the display.

Table 110 show crypto mib ipsec flowmib endpoint Field Descriptions

Field	Description
Index	The number of the endpoint associated with the IPsec phase-2 tunnel table. The value of this index is a number which begins at one and is incremented with each endpoint associated with an IPsec phase-2 tunnel. The index value will wrap at 2,147,483,647.
Local type	The local endpoint identity type. The three possible values are a single IP address, an IP address range, or an IP subnet.
Local address	The first IP address of the local endpoint. If the local endpoint type is a single IP address, then the local address is the value of the IP address. If the local endpoint type is an IP address range, then the local address is the value of beginning IP address of the range. If the local endpoint type is an IP subnet, then the local address is the value of the subnet.
Protocol	The local endpoint traffic protocol number.
Local port	The local endpoint traffic port number.
Remote type	The remote endpoint identity type. The three possible values are a single IP address, an IP address range, or an IP subnet.
Remote address	The first IP address of the remote endpoint. If the remote endpoint type is a single IP address, then the remote address is the value of the IP address. If the remote endpoint type is an IP address range, then the remote address is the value of beginning IP address of the range. If the remote endpoint type is an IP subnet, then the remote address is the value of the subnet.
Remote port	The remote endpoint traffic port number.

Related Commands

Command	Description
show crypto mib ipsec flowmib failure	Displays statistics associated with IPsec phase-2 failure.
show crypto mib ipsec flowmib global	Displays IPsec phase-2 global statistics.
show crypto mib ipsec flowmib history	Displays statistics associated with previously active IPsec phase-2 tunnels.
show crypto mib ipsec flowmib spi	Displays the IPsec phase-2 security protection index (SPI) table.
show crypto mib ipsec flowmib tunnel	Displays statistics for all active IPsec phase-2 tunnels.

show crypto mib ipsec flowmib failure

To display statistics associated with IP Security (IPsec) phase-2 failure, use the **show crypto mib ipsec flowmib failure** command in privileged EXEC mode.

show crypto mib ipsec flowmib failure [**vrf** *vrf-name*]

Syntax Description

vrf *vrf-name*	(Optional) Displays the parameters for the specified Virtual Private Network (VPN) routing and forwarding (VRF) instance.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(20)T	This command was introduced.
Cisco IOS XE Release 2.4	This command was implemented on the Cisco ASR 1000 series routers.

Examples

The following example displays the IPsec phase 2 MIB failure table for all indexes and VRFs:

```
Router# show crypto mib ipsec flowmib failure

vrf Global
  Index:                        1
  Reason:                       Operation request
  Failure time since reset:     00:25:18
  Src address:                  192.1.2.1
  Destination address:          192.1.2.2
  SPI:                          0
```

Table 111 describes the significant fields shown in the display.

Table 111 show crypto mib ipsec flowmib failure Field Descriptions

Field	Description
Index	The IPsec phase-2 failure table index. The value of the index is a number that begins at one and is incremented with each IPsec phase-1 failure. The index value will wrap at 2,147,483,647.
Reason	The reason for the failure, which are: • 1—All other reasons. • 2—An internal error occurred. • 3—A peer encoding error occurred. • 4—A proposal failure occurred. • 5—A protocol use failure occurred. • 6—The SA did not exist. • 7—A decryption failure occurred. • 8—An encryption failure occurred. • 9—An inbound authentication failure occurred. • 10—An outbound authentication failure occurred. • 11—A compression failure occurred. • 12—A system capacity failure occurred. • 13—A peer delete request was received. • 14—The contact with the peer was lost. • 15—The sequence rolled over. • 16—The operator requested tunnel termination.
Failure time since reset	The value of sysUpTime in hundredths of seconds at the time of the failure

Related Commands

Command	Description
show crypto mib ipsec flowmib endpoint	Displays IPsec phase-2 tunnel endpoint table.
show crypto mib ipsec flowmib global	Displays IPsec phase-2 global statistics.
show crypto mib ipsec flowmib history	Displays statistics associated with previously active IPsec phase-2 tunnels.
show crypto mib ipsec flowmib spi	Displays the IPsec phase-2 SPI table.
show crypto mib ipsec flowmib tunnel	Displays statistics for all active IPsec phase-2 tunnels.

show crypto mib ipsec flowmib global

To display IP Security (IPsec) phase-2 global statistics, use the **show crypto mib ipsec flowmib global** command in privileged EXEC mode.

show crypto mib ipsec flowmib global [**vrf** *vrf-name*]

Syntax Description

vrf *vrf-name*	(Optional) Displays the parameters for the specified Virtual Private Network (VPN) routing and forwarding (VRF) instance.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(20)T	This command was introduced.
Cisco IOS XE Release 2.4	This command was implemented on the Cisco ASR 1000 series routers.

Examples

The following example displays IPsec phase 2 global statistics for all VRFs:

```
Router# show crypto mib ipsec flowmib global

 vrf Global
  Active Tunnels:                   2
  Previous Tunnels:                 0
  In octets:                        800
  Out octets:                       1408
  In packets:                       8
  Out packets:                      8
  Uncompressed encrypted bytes:     1408
  In packets drops:                 0
  Out packets drops:                2
  In replay drops:                  0
  In authentications:               8
  Out authentications:              8
  In decrypts:                      8
  Out encrypts:                     8
  Compressed bytes:                 0
  Uncompressed bytes:               0
  In uncompressed bytes:            0
  Out uncompressed bytes:           0
  In decrypt failures:              0
  Out encrypt failures:             0
  No SA failures:                   0
  Protocol use failures:            0
  System capacity failures:         0
  In authentication failures:          0
  Out authentication failures:         0
```

Table 112 describes the significant fields shown in the display.

Table 112 show crypto mib ipsec flowmib global Field Descriptions

Field	Description
Active Tunnels	The total number of currently active IPsec phase-2 tunnels.
Previous Tunnels	The total number of previously active IPsec phase-2 tunnels.
In octets	The total number of octets received by all current and previous IPsec phase-2 tunnels. The total number is accumulated before determining whether or not the packet should be decompressed.
Out octets	The total number of octets sent by all current and previous IPsec phase-2 Tunnels. The total number is accumulated after determining whether or not the packet should be compressed.
In packets drops	The total number of packets dropped during receive processing by all current and previous IPsec phase-2 tunnels. The total number does not include packets dropped due to anti-replay processing.
Out packets drops	The total number of packets dropped during send processing by all current and previous IPsec phase-2 tunnels.
In replay drops	The total number of packets dropped during receive processing due to anti-replay processing by all current and previous IPsec phase-2 tunnels.
No SA failures	The total number of non-existent SA inbound failures that occurred during processing of all current and previous IPsec phase-2 tunnels.

Related Commands

Command	Description
show crypto mib ipsec flowmib endpoint	Displays IPsec phase-2 tunnel endpoint table.
show crypto mib ipsec flowmib failure	Displays statistics associated with IPsec phase-2 failure.
show crypto mib ipsec flowmib history	Displays statistics associated with previously active IPsec phase-2 tunnels.
show crypto mib ipsec flowmib spi	Displays the IPsec phase-2 SPI table.
show crypto mib ipsec flowmib tunnel	Displays statistics for all active IPsec phase-2 tunnels.

show crypto mib ipsec flowmib history

To display statistics associated with previously active IP Security (IPsec) phase-2 tunnels, use the **show crypto mib ipsec flowmib history** command in privileged EXEC mode.

show crypto mib ipsec flowmib history [**vrf** *vrf-name*]

Syntax Description

vrf *vrf-name*	(Optional) Displays the parameters for the specified Virtual Private Network (VPN) routing and forwarding (VRF) instance.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(20)T	This command was introduced.
Cisco IOS XE Release 2.4	This command was implemented on the Cisco ASR 1000 series routers.

Examples

The following example displays the IPsec phase 2 history statistics for all VRFs:

```
Router# show crypto mib ipsec flowmib history

vrf Global
  Reason:                       Operation request
  Index:                        1
  Local address:                192.1.2.1
  Remote address:               192.1.2.2
  IPSEC keying:                 IKE
  Encapsulation mode:           1
  Lifetime (KB):                4608000
  Lifetime (Sec):               3600
  Active time:                  00:24:32
  Lifetime threshold (KB):      423559168
  Lifetime threshold (Sec):     3590000
  Total number of refreshes:    0
  Expired SA instances:         4
  Current SA instances:         4
  In SA DH group:               1
  In sa encrypt algorithm       des
  In SA auth algorithm:         rsig
  In SA ESP auth algo:          ESP_HMAC_SHA
  In SA uncompress algorithm:   None
  Out SA DH group:              1
  Out SA encryption algorithm:  des
  Out SA auth algorithm:        ESP_HMAC_SHA
  Out SA ESP auth algorithm:    ESP_HMAC_SHA
  Out SA uncompress algorithm:  None
  In octets:                    400
  Decompressed octets:          400
  In packets:                   4
  In drops:                         0
  In replay drops:                  0
  In authentications:               4
```

```
In authentication failures:      0
In decrypts:                     4
In decrypt failures:             0
Out octets:                      704
Out uncompressed octets:         704
Out packets:                     4
Out drops:                       1
Out authentications:             4
Out authentication failures:     0
Out encryptions:                 4
Out encryption failures:         0
Compressed octets:               0
Decompressed octets:             0
Out uncompressed octets:         704
```

Table 113 describes the significant fields shown in the display.

Table 113 show crypto mib ipsec flowmib history Field Descriptions

Field	Description
Reason	The reason the IPsec phase-2 tunnel was terminated, which are: • 1—All other reasons. • 2—The tunnel terminated normally. • 3—The operator requested the tunnel termination. • 4—A peer delete request was received. • 5—The contact with peer was lost. • 6—A local failure occurred. • 7—The operator initiated a check point request.
Index	The index of the IPsec phase-2 tunnel history table. The value of the index is an integer that begins at one and is incremented with each tunnel that ends. The index value will wrap at 2,147,483,647.
IPSEC keying	The type of key used by the IPsec phase-2 tunnel.
Total number of refreshes	The total number of SA refreshes performed.
In octets	The total number of octets received by the IPsec phase-2 tunnel. The value is accumulated before determining whether or not the packet should be decompressed.
In drops	The total number of packets dropped during receive processing by this IPsec phase-2 tunnel. The number of drops does not include packets dropped due to anti-replay processing.
In replay drops	The total number of packets dropped during receive processing due to anti-replay processing by the IPsec phase-2 tunnel.

Related Commands

Command	Description
show crypto mib ipsec flowmib endpoint	Displays IPsec phase-2 tunnel endpoint table.
show crypto mib ipsec flowmib failure	Displays statistics associated with IPsec phase-2 failure.
show crypto mib ipsec flowmib global	Displays IPsec phase-2 global statistics.
show crypto mib ipsec flowmib spi	Displays the IPsec phase-2 SPI table.
show crypto mib ipsec flowmib tunnel	Displays statistics for all active IPsec phase-2 tunnels.

show crypto mib ipsec flowmib history failure size

To display the size of the IP Security (IPSec) failure history table, use the **show crypto mib ipsec flowmib history failure size** command in privileged EXEC mode.

show crypto mib ipsec flowmib history failure size

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.1(4)E	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **show crypto mib ipsec flowmib history failure size** command to display the size of the failure history table.

Examples

The following is sample output from the **show crypto mib ipsec flowmib history failure size** command:

```
Router# show crypto mib ipsec flowmib history failure size

IPSec Failure Window size: 140
```

Related Commands

Command	Description
crypto mib ipsec flowmib history failure size	Changes the size of the IPSec failure history table.
show crypto mib ipsec flowmib version	Displays the IPSec Flow MIB version used by the router.

show crypto mib ipsec flowmib history tunnel size

To display the size of the IP Security (IPSec) tunnel history table, use the **show crypto mib ipsec flowmib history tunnel size** command in privileged EXEC mode.

show crypto mib ipsec flowmib history tunnel size

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.1(4)E	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **show crypto mib ipsec flowmib history tunnel size** command to display the size of the tunnel history table.

Examples

The following is sample output from the **show crypto mib ipsec flowmib history tunnel size** command:

```
Router# show crypto mib ipsec flowmib history tunnel size

IPSec History Window Size: 130
```

Related Commands

Command	Description
crypto mib ipsec flowmib history tunnel size	Changes the size of the IPSec tunnel history table.
show crypto mib ipsec flowmib version	Displays the IPSec Flow MIB version used by the router.

show crypto mib ipsec flowmib spi

To display the IP Security (IPsec) phase-2 security protection index (SPI) table, use the **show crypto mib ipsec flowmib spi** command in privileged EXEC mode.

show crypto mib ipsec flowmib spi [**vrf** *vrf-name*]

Syntax Description

vrf *vrf-name*	(Optional) Displays the parameters for the specified Virtual Private Network (VPN) routing and forwarding (VRF) instance.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(20)T	This command was introduced.
Cisco IOS XE Release 2.4	This command was implemented on the Cisco ASR 1000 series routers.

Usage Guidelines

The IPsec phase-2 SPI table contains an entry for each active and expiring security association (SA).

Examples

The following example displays the IPsec phase-2 SPI table for all VRFs:

```
Router# show crypto mib ipsec flowmib spi

vrf Global
 Tunnel Index:          1
  SPI Index:            1
  SPI Value:            0xCC57D053
  SPI Direction:        In
  SPI Protocol:         AH
  SPI Status:           Active

  SPI Index:            2
  SPI Value:            0x68612DF
  SPI Direction:        Out
  SPI Protocol:         AH
  SPI Status:           Active

  SPI Index:            3
  SPI Value:            0x56947526
  SPI Direction:        In
  SPI Protocol:         ESP
  SPI Status:           Active

  SPI Index:            4
  SPI Value:            0x8D7C2204
  SPI Direction:        Out
  SPI Protocol:         ESP
  SPI Status:           Active
```

The field descriptions in the display are self-explanatory.

Related Commands

Command	Description
show crypto mib ipsec flowmib endpoint	Displays IPsec phase-2 tunnel endpoint table.
show crypto mib ipsec flowmib failure	Displays statistics associated with IPsec phase-2 failure.
show crypto mib ipsec flowmib global	Displays IPsec phase-2 global statistics.
show crypto mib ipsec flowmib history	Displays statistics associated with previously active IPsec phase-2 tunnels.
show crypto mib ipsec flowmib tunnel	Displays statistics for all active IPsec phase-2 tunnels.

show crypto mib ipsec flowmib tunnel

To display statistics for all active IP Security (IPsec) phase-2 tunnels, use the **show crypto mib ipsec flowmib tunnel** command in privileged EXEC mode.

show crypto mib ipsec flowmib tunnel [**index** *tunnel-mib-index*] [**vrf** *vrf-name*]

Syntax Description

vrf *vrf-name*	(Optional) Displays the parameters for the specified Virtual Private Network (VPN) routing and forwarding (VRF) instance.
index *tunnel-mib-index*	(Optional) Displays tunnel MIB information for the specified active tunnel. The tunnel MIB index is an integer, 0–65535.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(20)T	This command was introduced.
Cisco IOS XE Release 2.4	This command was implemented on the Cisco ASR 1000 series routers.

Examples

The following example displays statistics for all active IPsec phase-2 tunnels for all tunnel indexes and VRFs:

```
Router# show crypto mib ipsec flowmib tunnel

vrf Global
  Index:                            1
  Local address:                    192.0.2.1
  Remote address:                   192.0.2.2
  IPSEC keying:                     IKE
  Encapsulation mode:               1
  Lifetime (KB):                    4608000
  Lifetime (Sec):                   3600
  Active time:                      00:05:46
  Lifetime threshold (KB):          64
  Lifetime threshold (Sec):         10
  Total number of refreshes:        0
  Expired SA instances:             0
  Current SA instances:             4
  In SA DH group:                   1
  In sa encrypt algorithm:          des
  In SA auth algorithm:             rsig
  In SA ESP auth algo:              ESP_HMAC_SHA
  In SA uncompress algorithm:       None
  Out SA DH group:                  1
  Out SA encryption algorithm:      des
  Out SA auth algorithm:            ESP_HMAC_SHA
  Out SA ESP auth algorithm:        ESP_HMAC_SHA
  Out SA uncompress algorithm:      None
  In octets:                           400
```

```
Decompressed octets:                  400
In packets:                           4
In drops:                             0
In replay drops:                      0
In authentications:                   4
In authentication failures:           0
In decrypts:                          4
In decrypt failures:                  0
Out octets:                           704
Out uncompressed octets:              704
Out packets:                          4
Out drops:                            1
Out authentications:                  4
Out authentication failures:          0
Out encryptions:                      4
Out encryption failures:              0
Compressed octets:                    0
Decompressed octets:                  0
Out uncompressed octets:              704
```

Table 114 describes the significant fields shown in the display.

Table 114 show crypto mib ipsec flowmib tunnel Field Descriptions

Field	Description
Index	The index of the IPsec phase-2 tunnel table. The index value is an integer that begins at one and is incremented with each tunnel that is created. The index value will wrap at 2,147,483,647.
Total number of refreshes	The total number of SA refreshes performed.
Current SA instances	The number of SA instances that are currently active or expiring.
In octets	The total number of octets received by the IPsec phase-2 tunnel. This total number is accumulated before determining whether or not the packet should be decompressed.
Decompressed octets	The total number of decompressed octets received by the IPsec phase-2 tunnel. The total number is accumulated after the packet is decompressed. If compression is not being used, the total number will match the value of cipSecTunInOctets.
In drops	The total number of packets dropped during receive processing by the IPsec phase-2 tunnel. This count does not include packets dropped due to anti-replay processing.
In replay drops	The total number of packets dropped during receive processing due to anti-replay processing by the IPsec phase-2 tunnel.
Out octets	The total number of octets sent by the IPsec phase-2 tunnel. This value is accumulated after determining whether or not the packet should be compressed.

Related Commands

Command	Description
show crypto mib ipsec flowmib endpoint	Displays IPsec phase-2 tunnel endpoint table.
show crypto mib ipsec flowmib failure	Displays statistics associated with IPsec phase-2 failure.
show crypto mib ipsec flowmib global	Displays IPsec phase-2 global statistics.
show crypto mib ipsec flowmib history	Displays statistics associated with previously active IPsec phase-2 tunnels.
show crypto mib ipsec flowmib spi	Displays the IPsec phase-2 SPI table.

show crypto mib ipsec flowmib version

To display the IP Security (IPSec) MIB version used by the router, use the **show crypto mib ipsec flowmib version** command in privileged EXEC mode.

show crypto mib ipsec flowmib version

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.1(4)E	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **show crypto mib ipsec flowmib version** command to display the MIB version used by the management applications to identify the feature set.

Note The MIB version can also be obtained by querying the MIB element cipSecMibLevel using Simple Network Management Protocol (SNMP).

Examples

The following is sample output from the **show crypto mib ipsec flowmib version** command:

```
Router# show crypto mib ipsec flowmib version

IPSec Flow MIB version: 1
```

Related Commands

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

show crypto mib isakmp flowmib failure

To display the statistics associated with an Internet Security Association and Key Management Protocol (ISAKMP) phase-1 failure, use the **show crypto mib isakmp flowmib failure** command in privileged EXEC mode.

show crypto mib isakmp flowmib failure [**vrf** *vrf-name*]

Syntax Description

vrf *vrf-name*	(Optional) Displays the parameters for a specific Virtual Private Network (VPN) routing and forwarding (VRF) instance.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(20)T	This command was introduced.
Cisco IOS XE Release 2.4	This command was implemented on the Cisco ASR 1000 series routers.

Examples

The following is sample output from the **show crypto mib isakmp flowmib failure** command:

```
vrf Global
 Index:                        1
 Reason:                       peer lost
 Failure time since reset:     00:07:27
 Local type:                   ID_IPV4_ADDR
 Local value:                 192.0.2.1
 Remote type:                  ID_IPV4_ADDR
 Remote Value:                 192.0.2.2
 Local Address:                192.0.2.1
 Remote Address:               192.0.2.2
 Index:                        2
 Reason:                       peer lost
 Failure time since reset:     00:07:27
 Local type:                   ID_IPV4_ADDR
 Local value:                 192.0.3.1
 Remote type:                  ID_IPV4_ADDR
 Remote Value:                 192.0.3.2
 Local Address:                192.0.3.1
 Remote Address:               192.0.3.2
 Index:                        3
 Reason:                       peer lost
 Failure time since reset:     00:07:32
 Local type:                   ID_IPV4_ADDR
 Remote type:                  ID_IPV4_ADDR
 Remote Value:                 192.0.2.2
 Local Address:                192.0.2.1
 Remote Address:               192.0.2.2
```

Table 115 describes the significant fields shown in the display.

Table 115 show crypto mib isakmp flowmib failure Field Descriptions

Field	Description
Index	The IPsec phase-1 failure table index. The value of the index is a number that begins at one and is incremented with each IPsec phase-1 failure. The index value will wrap at 2,147,483,647.
Reason	The reason for the failure, which include: • 1—All other reasons. • 2—A peer delete request was received. • 3—The contact with peer was lost. • 4—A local failure occurred. • 5—An authentication failure occurred. • 6—A hash validation failure occurred. • 7—An encryption failure occurred. • 8—An internal error occurred. • 9—A system capacity failure occurred. • 10—A proposal failure occurred. • 11—The peer certificate was unavailable. • 12—The peer certificate was invalid. • 13—The local certificate expired. • 14—A certificate revoke list (CRL) failure occurred. • 15—A peer encoding error occurred. • 16—The SA did not exist. • 17—The operator requested tunnel termination.
Failure time since reset	The value of sysUpTime in hundredths of seconds at the time of the failure.
Local type	The type of local peer identity. • 1—Indicates an IP address identity type. • 2—Indicates a hostname identity type.
Local value	The value of the local peer identity. If the local peer type is an IP address, then the value is the IP address used to identify the local peer. If the local peer type is a hostname, then the value is the hostname used to identify the local peer.
Remote type	The type of remote peer identity. • 1—Indicates an IP address identity type. • 2—Indicates a hostname identity type.

Table 115 show crypto mib isakmp flowmib failure Field Descriptions (continued)

Field	Description
Remote Value	The value of the remote peer identity. If the remote peer type is an IP address, then the value is the IP address used to identify the remote peer. If the remote peer type is a hostname, then the value is the hostname used to identify the remote peer.
Local Address	The IP address of the local peer.
Remote Address	The IP address of the remote peer.

Related Commands

Command	Description
show crypto ipsec transform-set	Displays configured IPsec transform sets.
show crypto map	Displays IPsec crypto map configurations.
show crypto mib isakmp flowmib global	Displays global ISAKMP statistics.
show crypto mib isakmp flowmib history	Displays statistics associated with previously active ISAKMP tunnels.
show crypto mib isakmp flowmib peer	Displays attributes for an ISKMP peer association.
show crypto mib isakmp flowmib tunnel	Displays statistics associated with active ISAKMP tunnels.

show crypto mib isakmp flowmib global

To display the global Internet Security Association and Key Management Protocol (ISAKMP) phase-1 statistics, use the **show crypto mib isakmp flowmib global** command in privileged EXEC mode.

show crypto mib isakmp flowmib global [**vrf** *vrf-name*]

Syntax Description

vrf *vrf-name*	(Optional) Displays the parameters for a specific Virtual Private Network (VPN) routing and forwarding (VRF) instance.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(20)T	This command was introduced.
Cisco IOS XE Release 2.4	This command was implemented on the Cisco ASR 1000 series routers.

Examples

The following example displays global ISAKMP statistics:

```
Router# show crypto mib isakmp flowmib global

vrf Global
  Active Tunnels:                       3
  Previous Tunnels:                     0
  In octets:                            2856
  Out octets:                           3396
  In packets:                           16
  Out packets:                          19
  In packets drop:                      0
  Out packets drop:                     0
  In notifys:                           4
  Out notifys:                          7
  In P2 exchg:                          3
  Out P2 exchg:                         6
  In P2 exchg invalids:                 0
  Out P2 exchg invalids:                0
  In P2 exchg rejects:                  0
  Out P2 exchg rejects:                 0
  In IPSEC delete:                      0
  Out IPSEC delete:                     0
  SAs locally initiated:                3
  SAs locally initiated failed:         0
  SAs remotely initiated failed:        0
  System capacity failures:             0
  Authentication failures:              0
  Decrypt failures:                     0
  Hash failures:                        0
  Invalid SPI:                          0
```

Table 116 describes the fields shown in the display.

Table 116 show crypto mib isakmp flowmib global Field Descriptions

Field	Description
Active Tunnels	The number of currently active IPsec phase-1 IKE tunnels.
Previous Tunnels	The total number of previously active IPsec phase-1 IKE tunnels.
In octets	The total number of octets received by all currently and previously active IPsec phase-1 IKE tunnels.
Out octets	The total number of octets sent by all currently and previously active and IPsec phase-1 IKE tunnels.
In packets	The total number of packets received by all currently and previously active IPsec phase-1 IKE tunnels.
Out packets	The total number of packets sent by all currently and previously active and IPsec phase-1 tunnels.
In packets drop	The total number of packets that were dropped during receive processing by all currently and previously active IPsec phase-1 IKE tunnels.
Out packets drop	The total number of packets that were dropped during send processing by all currently and previously active IPsec phase-1 IKE tunnels.
In notifys	The total number of notifications received by all currently and previously active IPsec phase-1 IKE tunnels.
Out notifys	The total number of notifications sent by all currently and previously active IPsec phase-1 IKE tunnels.
In P2 exchg	The total number of IPsec phase-2 exchanges received by all currently and previously active IPsec phase-1 IKE tunnels.
Out P2 exchg	The total number of IPsec phase-2 exchanges that were sent by all currently and previously active IPsec phase-1 IKE tunnels.
In P2 exchg invalids	The total number of IPsec phase-2 exchanges that were received and found to be invalid by all currently and previously active IPsec phase-1 IKE tunnels.
Out P2 exchg invalids	The total number of IPsec phase-2 exchanges that were sent and found to be invalid by all currently and previously active IPsec phase-1 tunnels.
In P2 exchg rejects	The total number of IPsec phase-2 exchanges that were received and rejected by all currently and previously active IPsec phase-1 IKE tunnels.
Out P2 exchg rejects	The total number of IPsec phase-2 exchanges that were sent and rejected by all currently and previously active IPsec phase-1 IKE tunnels.
In IPSEC delete	The total number of IPsec phase-2 SA delete requests received by all currently and previously active and IPsec phase-1 IKE tunnels.

Table 116 show crypto mib isakmp flowmib global Field Descriptions (continued)

Field	Description
Out IPSEC delete	The total number of IPsec phase-2 SA delete requests sent by all currently and previously active IPsec phase-1 IKE tunnels.
SAs locally initiated	The total number of IPsec phase-1 IKE tunnels that were locally initiated.
SAs locally initiated failed	The total number of IPsec phase-1 IKE tunnels that were locally initiated and failed to activate.
SAs remotely initiated failed	The total number of IPsec phase-1 IKE tunnels that were remotely initiated and failed to activate.
System capacity failures	The total number of system capacity failures that occurred during processing of all current and previously active IPsec phase-1 IKE tunnels.
Authentication failures	The total number of authentications that ended in failure by all current and previous IPsec phase-1 IKE tunnels.
Decrypt failures	The total number of decryptions that ended in failure by all current and previous IPsec phase-1 IKE tunnels.
Hash failures	The total number of hash validations that ended in failure by all current and previous IPsec phase-1 IKE tunnels.
Invalid SPI	The total number of non-existent SAs in failures which occurred during processing of all current and previous IPsec phase-1 IKE tunnels.

Related Commands

Command	Description
show crypto mib isakmp flowmib failure	Displays statistics associated with an ISAKMP failure.
show crypto mib isakmp flowmib history	Displays statistics associated with previously active ISAKMP tunnels.
show crypto mib isakmp flowmib peer	Displays attributes for an ISKMP peer association.
show crypto mib isakmp flowmib tunnel	Displays statistics associated with active ISAKMP tunnels.

show crypto mib isakmp flowmib history

To display the statistics associated with previously active Internet Security Association and Key Management Protocol (ISAKMP) phase-1 tunnels, use the **show crypto mib isakmp flowmib history** command in privileged EXEC mode.

show crypto mib isakmp flowmib history [**vrf** *vrf-name*]

Syntax Description

vrf *vrf-name*	(Optional) Displays the parameters for a specific Virtual Private Network (VPN) routing and forwarding (VRF) instance.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(20)T	This command was introduced.
Cisco IOS XE Release 2.4	This command was implemented on the Cisco ASR 1000 series routers.

Examples

The following example displays previous ISAKMP phase-1 tunnel information for all VRFs:

```
Router# show crypto mib isakmp flowmib history

vrf Global
  Reason:                          peer lost
  Index:                           2
  Local type:                      ID_IPV4_ADDR
  Local address:                   192.0.2.1
  Remote type:                     ID_IPV4_ADDR
  Remote address:                  192.0.2.2
  Negotiation mode:                Main Mode
  Diffie Hellman Grp:              2
  Encryption algo:                 des
  Hash algo:                       sha
  Auth method:                     psk
  Lifetime:                        86400
  Active time:                     00:06:30
  Policy priority:                 1
  Keepalive enabled:               Yes
  In octets:                       3024
  In packets:                      22
  In drops:                        0
  In notifys:                      18
  In P2 exchanges:                 1
  In P2 exchg invalids:            0
  In P2 exchg rejected:              0
  In P2 SA delete reqs:              0
  Out octets:                        4188
  Out packets:                       33
  Out drops:                         0
  Out notifys:                       28
  Out P2 exchgs:                     2
```

```
Out P2 exchg invalids:              0
Out P2 exchg rejects:               0
Out P2 Sa delete requests:          0
Reason:                             peer lost
Index:                              3
Local type:                         ID_IPV4_ADDR
Local address:                      192.0.3.1
Remote type:                        ID_IPV4_ADDR
Remote address:                     192.0.3.2
Negotiation mode:                   Main Mode
Diffie Hellman Grp:                 2
Encryption algo:                    des
Hash algo:                          sha
Auth method:                        psk
Lifetime:                           86400
Active time:                        00:06:25
Policy priority:                    1
Keepalive enabled:                  Yes
In octets:                          3140
In packets:                         23
In drops:                           0
In notifys:                         19
In P2 exchanges:                    1
In P2 exchg invalids:               0
In P2 exchg rejected:               0
In P2 SA delete reqs:               0
Out octets:                         4304
Out packets:                        34
Out drops:                          0
Out notifys:                        29
Out P2 exchgs:                      2
Out P2 exchg invalids:              0
Out P2 exchg rejects:               0
Out P2 Sa delete requests:          0
```

Table 117 describes the significant fields shown in the display.

Table 117 show crypto mib isakmp flowmib history Field Descriptions

Field	Description
Reason	The reason the IPsec phase-1 IKE tunnel was terminated, which include: • 1—All other reasons. • 2—The tunnel terminated normally. • 3—The operator requested tunnel termination. • 4—A peer delete request was received. • 5—The contact with peer was lost. • 6—A local failure occurred. • 7—The operator initiated a check point request.
Index	The index of the IPsec phase-1 IKE tunnel history table. The value of the index is a number that begins at one and is incremented with each tunnel that ends. The value of this object will wrap at 2,147,483,647.

Table 117 show crypto mib isakmp flowmib history Field Descriptions (continued)

Field	Description
Local type	The type of local peer identity. • 1—Indicates an IP address identity type. • 2—Indicates a hostname identity type.
Local address	The value of the local peer identity. If the local peer type is an IP address, then the value is the IP address used to identify the local peer. If the local peer type is a hostname, then the value is the hostname used to identify the local peer.
Remote type	The type of remote peer identity. • 1—Indicates an IP address identity type. • 2—Indicates a hostname identity type.
Remote address	The value of the remote peer identity. If the remote peer type is an IP address, then the value is the IP address used to identify the remote peer. If the remote peer type is a hostname, then the value is the hostname used to identify the remote peer.
Lifetime	The negotiated lifetime of the IPsec phase-1 IKE tunnel in seconds.
Active time	The length of time the IPsec phase-1 IKE tunnel has been active in hundredths of seconds.
In octets	The total number of octets received by all currently and previously active IPsec phase-1 IKE tunnels.
In packets	The total number of packets received by all currently and previously active IPsec phase-1 IKE tunnels.
In drops	The total number of packets that were dropped during receive processing by all currently and previously active IPsec phase-1 IKE tunnels.
In notifys	The total number of notifications received by all currently and previously active IPsec phase-1 IKE tunnels.
In P2 exchanges	The total number of IPsec phase-2 exchanges received by all currently and previously active IPsec phase-1 IKE tunnels.
In P2 exchg invalids	The total number of IPsec phase-2 exchanges that were received and found to be invalid by all currently and previously active IPsec phase-1 IKE tunnels.
In P2 exchg rejected	The total number of IPsec phase-2 exchanges that were received and rejected by all currently and previously active IPsec phase-1 IKE tunnels.
In P2 SA delete reqs	The total number of IPsec phase-2 SA delete requests received by all currently and previously active and IPsec phase-1 IKE tunnels.
Out octets	The total number of octets sent by all currently and previously active and IPsec phase-1 IKE tunnels.

Table 117 show crypto mib isakmp flowmib history Field Descriptions (continued)

Field	Description
Out packets	The total number of packets sent by all currently and previously active and IPsec phase-1 tunnels.
Out drops	The total number of packets that were dropped during send processing by all currently and previously active IPsec phase-1 IKE tunnels.
Out notifys	The total number of notifications sent by all currently and previously active IPsec phase-1 IKE tunnels.
Out P2 exchgs	The total number of IPsec phase-2 exchanges that were sent by all currently and previously active IPsec phase-1 IKE tunnels.
Out P2 exchg invalids	The total number of IPsec phase-2 exchanges that were sent and found to be invalid by all currently and previously active IPsec phase-1 tunnels.
Out P2 exchg rejects	The total number of IPsec phase-2 exchanges that were sent and rejected by all currently and previously active IPsec phase-1 IKE tunnels.
Out P2 Sa delete requests	The total number of IPsec phase-2 SA delete requests sent by all currently and previously active IPsec phase-1 IKE tunnels.

Related Commands

Command	Description
show crypto mib isakmp flowmib failure	Displays statistics associated with an ISAKMP failure.
show crypto mib isakmp flowmib global	Displays global ISAKMP statistics.
show crypto mib isakmp flowmib peer	Displays attributes for an ISKMP peer association.
show crypto mib isakmp flowmib tunnel	Displays statistics associated with active ISAKMP tunnels.

show crypto mib isakmp flowmib peer

To display attributes for an active Internet Security Association and Key Management Protocol (ISAKMP) phase-1 peer association, use the **show crypto mib isakmp flowmib peer** command in privileged EXEC mode.

show crypto mib isakmp flowmib peer [**index** *peer-mib-index*] [**vrf** *vrf-name*]

Syntax Description

index *peer-mib-index*	(Optional) Displays MIB information for the specified peer. The peer MIB index is an integer, 0–65535.
vrf *vrf-name*	(Optional) Displays the parameters for the specified Virtual Private Network (VPN) routing and forwarding (VRF) instance.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(20)T	This command was introduced.
Cisco IOS XE Release 2.4	This command was implemented on the Cisco ASR 1000 series routers.

Examples

The following example displays ISAKMP peer information for all indexes and VRFs:

```
Router# show crypto mib isakmp flowmib peer

 vrf Global
  Index:              1
  Local type:         ID_IPV4_ADDR
  Local address:      192.0.2.1
  Remote type:        ID_IPV4_ADDR
  Remote address:     192.0.2.2

  Index:              2
  Local type:         ID_IPV4_ADDR
  Local address:      192.0.3.1
  Remote type:        ID_IPV4_ADDR
  Remote address:     192.0.3.1

  Index:              3
  Local type:         ID_IPV4_ADDR
  Local address:      192.0.4.1
  Remote type:        ID_IPV4_ADDR
  Remote address:     192.0.4.1
```

Table 118 describes the significant fields shown in the display.

Table 118 show crypto mib isakmp flowmib peer Field Descriptions

Field	Description
Index	The index of the active IPsec phase-1 IKE tunnel for this peer association. If an IPsec phase-1 IKE tunnel is not currently active, then the value of this object will be zero.
Local type	The type of local peer identity. • 1—Indicates an IP address identity type. • 2—Indicates a hostname identity type.
Local address	The IP address of the local peer.
Remote type	The type of remote peer identity. • 1—Indicates an IP address identity type. • 2—Indicates a hostname identity type.
Remote address	The IP address of the remote peer.

Related Commands

Command	Description
show crypto mib isakmp flowmib failure	Displays statistics associated with an ISAKMP failure.
show crypto mib isakmp flowmib global	Displays global ISAKMP statistics.
show crypto mib isakmp flowmib history	Displays statistics associated with previously active ISAKMP tunnels.
show crypto mib isakmp flowmib tunnel	Displays statistics associated with active ISAKMP tunnels.

show crypto mib isakmp flowmib tunnel

To display statistics associated with active Internet Security Association and Key Management Protocol (ISAKMP) phase-1 tunnels, use the **show crypto mib isakmp flowmib tunnel** command in privileged EXEC mode.

show crypto mib isakmp flowmib tunnel [**index** *tunnel-mib-index*] [**vrf** *vrf-name*]

Syntax Description

index *tunnel-mib-index*	(Optional) Displays tunnel MIB information for the specified tunnel. The tunnel MIB index is an integer, 0–65535.
vrf *vrf-name*	(Optional) Displays the parameters for the specified Virtual Private Network (VPN) routing and forwarding (VRF) instance.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(20)T	This command was introduced.
Cisco IOS XE Release 2.4	This command was implemented on the Cisco ASR 1000 series routers.

Examples

The following example displays ISAKMP tunnel information for all indexes and VRFs:

```
Router# show crypto mib isakmp flowmib tunnel

vrf Global
  Index:                    1
  Local type:               ID_IPV4_ADDR
  Local address:            192.0.2.1
  Remote type:              ID_IPV4_ADDR
  Remote address:           192.0.2.2
  Negotiation mode:         Main Mode
  Diffie Hellman Grp:       2
  Encryption algo:          des
  Hash algo:                sha
  Auth method:              psk
  Lifetime:                 86400
  Active time:              00:03:08
  Policy priority:          1
  Keepalive enabled:        Yes
  In octets:                2148
  In packets:               15
  In drops:                 0
  In notifys:               11
  In P2 exchanges:          1
  In P2 exchg invalids:     0
  In P2 exchg rejected:     0
  In P2 SA delete reqs:     0
  Out octets:               2328
  Out packets:              16
  Out drops:                    0
```

```
Out notifys:                    12
Out P2 exchgs:                  2

Out P2 exchg invalids:          0
Out P2 exchg rejects:           0
Out P2 Sa delete requests:      0
```

Table 119 describes the significant fields shown in the display.

Table 119 show crypto mib isakmp flowmib tunnel Field Descriptions

Field	Description
Index	The index of the IPsec phase-1 IKE tunnel table. The value of the index is a number that begins at one and is incremented with each tunnel that is created. The value of this object will wrap at 2,147,483,647.
Local type	The type of local peer identity. • 1—Indicates an IP address identity type. • 2—Indicates a hostname identity type.
Local address	The value of the local peer identity. If the local peer type is an IP address, then the local address is the IP address used to identify the local peer. If the local peer type is a hostname, then the local address is the hostname used to identify the local peer.
Remote type	The type of remote peer identity. • 1—Indicates an IP address identity type. • 2—Indicates a hostname identity type.
Remote address	The value of the remote peer identity. If the remote peer type is an IP address, then the remote address is the IP address used to identify the remote peer. If the remote peer type is a hostname, then the remote address is the hostname used to identify the remote peer.
Negotiation mode	The negotiation mode of the IPsec phase-1 IKE tunnel.
Diffie Hellman Grp	The Diffie Hellman group used in IPsec phase-1 IKE negotiations.
Encryption algo	The encryption algorithm used in IPsec phase-1 IKE negotiations.
Hash algo	The hash algorithm used in IPsec phase-1 IKE negotiations.
Auth method	The authentication method used in IPsec phase-1 IKE negotiations.
Lifetime	The negotiated lifetime of the IPsec phase-1 IKE tunnel in seconds
Active time	The length of time the IPsec phase-1 IKE tunnel has been active in hundredths of seconds.
In octets	The total number of octets received by all currently and previously active IPsec phase-1 IKE tunnels.

Table 119 show crypto mib isakmp flowmib tunnel Field Descriptions (continued)

Field	Description
In packets	The total number of packets received by all currently and previously active IPsec phase-1 IKE tunnels.
In drops	The total number of packets that were dropped during receive processing by all currently and previously active IPsec phase-1 IKE tunnels.
In notifys	The total number of notifications received by all currently and previously active IPsec phase-1 IKE tunnels.
In P2 exchanges	The total number of IPsec phase-2 exchanges received by all currently and previously active IPsec phase-1 IKE tunnels.
In P2 exchg invalids	The total number of IPsec phase-2 exchanges that were received and found to be invalid by all currently and previously active IPsec phase-1 IKE tunnels.
In P2 exchg rejected	The total number of IPsec phase-2 exchanges that were received and rejected by all currently and previously active IPsec phase-1 IKE tunnels.
In P2 SA delete reqs	The total number of IPsec phase-2 SA delete requests received by all currently and previously active and IPsec phase-1 IKE tunnels.
Out octets	The total number of octets sent by all currently and previously active and IPsec phase-1 IKE tunnels.
Out packets	The total number of packets sent by all currently and previously active and IPsec phase-1 tunnels.
Out drops	The total number of packets that were dropped during send processing by all currently and previously active IPsec phase-1 IKE tunnels.
Out notifys	The total number of notifications sent by all currently and previously active IPsec phase-1 IKE tunnels.
Out P2 exchgs	The total number of IPsec phase-2 exchanges that were sent by all currently and previously active IPsec phase-1 IKE tunnels.
Out P2 exchg invalids	The total number of IPsec phase-2 exchanges that were sent and found to be invalid by all currently and previously active IPsec phase-1 tunnels.
Out P2 exchg rejects	The total number of IPsec phase-2 exchanges that were sent and rejected by all currently and previously active IPsec phase-1 IKE tunnels.
Out P2 Sa delete requests	The total number of IPsec phase-2 SA delete requests sent by all currently and previously active IPsec phase-1 IKE tunnels.

Related Commands

Command	Description
show crypto mib isakmp flowmib failure	Displays statistics associated with an ISAKMP failure.
show crypto mib isakmp flowmib global	Displays global ISAKMP statistics.
show crypto mib isakmp flowmib history	Displays statistics associated with previously active ISAKMP tunnels.
show crypto mib isakmp flowmib peer	Displays attributes for an ISKMP peer association.

show crypto pki benchmarks

To display benchmarking data for Public Key Infrastructure (PKI) performance monitoring and optimization that was collected, use the **show crypto pki benchmarks** command in privileged EXEC mode.

show crypto pki benchmarks [**failures**]

Syntax Description

failures	(Optional) Includes validation failures only.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(3)T	This command was introduced.

Usage Guidelines

Use the **show crypto pki benchmarks** command to display benchmarking data for PKI performance monitoring and optimization that was collected.

The IOS PKI Performance Monitoring and Optimization feature enables you to collect the following types of PKI performance data:

- Time to validate entire certificate chain.
- Time to verify each certificate.
- Time to check revocation status for each certificate.
- Time to fetch certificate revocation list (CRL) database for each fetch location.
- Time to fetch Simple Certificate Enrollment Protocol (SCEP) method capabilities to retrieve the CRL.
- Time to process each CRL.
- Time to process the Online Certificate Status Protocol (OCSP) response. OCSP is a certificate revocation mechanism.
- Time to fetch Authentication, Authorization, and Accounting (AAA).
- CRL size.
- Validation result.
- Validation Bypass (pubkey cached).
- Method used to fetch a CRL.
- PKI session identifier.
- Crypto engine used (hardware, software, etoken).

Examples

The following example displays **show crypto pki benchmark** command output of all PKI benchmarking data:

```
Router# show crypto pki benchmark

Display Validation Benchmark Table

 4 Records collected

Validation Session 10006
  Start: 20:47:29.021 GMT Wed Oct 27 2010
  Duration: 756 ms
  Peer Certificate Serial Number (hex): 296ED1EB0000000052FA
  Pubkey Bypass: no
  Result: Success
  Size of Chain to Validate: 1
  Revocation Check for Certificate 1 of 1
    Start: 20:47:29.063 GMT Wed Oct 27 2010
    Duration: 714 ms
  CRL Fetch - http://msca-root/CertEnroll/msca-root.crl
      Start: 20:47:29.067 GMT Wed Oct 27 2010
      Duration: 661 ms
      Fetch Result: Success
  CRL Insert
      Start: 20:47:29.731 GMT Wed Oct 27 2010
      Duration: 24 ms
  CRL Size: 582

Validation Session 10007
  Start: 20:48:15.897 GMT Wed Oct 27 2010
  Duration: 26 ms
  Pubkey Bypass: no
  Result: Failed CRYPTO_CERT_EXPIRED
  Size of Chain to Validate: 1

Validation Session 10008
  Start: 20:49:08.916 GMT Wed Oct 27 2010
  Duration: 26 ms
  Pubkey Bypass: no
  Result: Failed CRYPTO_CERT_EXPIRED
  Size of Chain to Validate: 1

Validation Session 10009
  Start: 20:49:15.051 GMT Wed Oct 27 2010
  Duration: 32 ms
  Peer Certificate Serial Number (hex): 296ED1EB0000000052FA
  Pubkey Bypass: no
  Result: Success
  Size of Chain to Validate: 1
  Revocation Check for Certificate 1 of 1
    Start: 20:49:15.076 GMT Wed Oct 27 2010
    Duration: 6 ms
```

The following example displays **show crypto pki benchmark** command output of a section filter in PKI benchmarking data:

```
Router# show crypto pki benchmark | section Revocation
  Revocation Check for Certificate 1 of 1
    Start: 20:47:29.063 GMT Wed Oct 27 2010
    Duration: 714 ms
  Revocation Check for Certificate 1 of 1
    Start: 20:49:15.076 GMT Wed Oct 27 2010
    Duration: 6 ms
```

Related Commands

Command	Description
clear crypto pki benchmark	Clears PKI benchmarking performance monitoring and optimization data and releases all memory associated with this data.
crypto pki benchmark	Starts or stops benchmarking data for PKI performance monitoring and optimization.

show crypto pki certificates

To display information about your certificate, the certification authority certificate (CA), and any registration authority (RA) certificates, use the **show crypto pki certificates** command in privileged EXEC mode.

show crypto pki certificates [*trustpoint-name* [**verbose**]]

Syntax Description

trustpoint-name	(Optional) Name of the trustpoint. Using this argument indicates that only certificates that are related to the trustpoint are to be displayed.
verbose	(Optional) More detailed information is to be displayed. **Note** The **verbose** keyword can be used only if a trustpoint name is entered.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.3 T	The **show crypto ca certificates** command was introduced.
12.2(13)T	The *trustpoint-name* argument was added.
12.3(7)T	This command replaced the **show crypto ca certificates** command.
12.3(8)T	The **verbose** keyword was added.
12.3(14)T	The command output was modified to include persistent self-signed certificate parameters.
12.4(2)T	The command output was modified to include shadow public key infrastructure (PKI), or rollover, certificate details.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(22)T	The command output was modified to include X.509 certificate IP address extension information.

Usage Guidelines

This command shows information about the following certificates:

- Your certificate, if you have requested one from the CA (see the **crypto pki enroll** command)
- The certificate of the CA, if you have received the certificate of the CA (see the **crypto pki authenticate** command)
- RA certificates, if you have received RA certificates (see the **crypto pki authenticate** command)
- A self-signed certificate, if one has been requested
- Shadow PKI, or rollover, certificate details, if one or more shadow PKI certificates exist

Examples

The following is sample output from the **show crypto pki certificates** command after you authenticated the CA by requesting the certificate of the CA and public key with the **crypto pki 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 pki certificates** command, and it shows the certificate of the router and the certificate of the CA. In this example, a single, general-purpose Rivest, Shamir, and Adelman (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 certificate status of the router 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 pki certificates** command, and it shows the certificates of two routers and the certificate of the CA. 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 pki certificates** command when the CA supports an RA. In this example, the CA and RA certificates were previously requested with the **crypto pki 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
```

The following is sample output from the **show crypto pki certificates** command using the optional *trustpoint-name* argument and **verbose** keyword. The output shows the certificate of a router and the certificate of the CA. In this example, general-purpose RSA key pairs were previously generated, and a certificate was requested and received for the key pair.

```
Certificate
   Status: Available
   Version: 3
   Certificate Serial Number: 18C1EE03000000004CBD
   Certificate Usage: General Purpose
   Issuer:
     cn=msca-root
     ou=pki msca-root
     o=company
     l=stown
     st=state
     c=US
     ea=user@example.com
   Subject:
     Name: myrouter.example.com
     hostname=myrouter.example.com
   CRL Distribution Points:
     http://msca-root/CertEnroll/msca-root.crl
   Validity Date:
     start date: 19:50:40 GMT Oct 5 2004
     end   date: 20:00:40 GMT Oct 12 2004
   Subject Key Info:
     Public Key Algorithm: rsaEncryption
     RSA Public Key: (360 bit)
   Signature Algorithm: SHA1 with RSA Encryption
   Fingerprint MD5: 2B5F53E6 E3E892E6 3A9D3706 01261F10
   Fingerprint SHA1: 315D127C 3AD34010 40CE7F3A 988BBDA5 CD528824
   X509v3 extensions:
     X509v3 Key Usage: A0000000
       Digital Signature
       Key Encipherment
     X509v3 Subject Key ID: D156E92F 46739CBA DFE66D2D 3559483E B41ECCF4
     X509v3 Authority Key ID: 37F3CC61 AF5E7C0B 434AB364 CF9FA0C1 B17C50D9
     Authority Info Access:
   Associated Trustpoints: msca-root
   Key Label: myrouter.example.com

CA Certificate
   Status: Available
   Version: 3
   Certificate Serial Number: 1244325DE0369880465F977A18F61CA8
   Certificate Usage: Signature
```

```
  Issuer:
    cn=msca-root
    ou=pki msca-root
    o=company
    l=town
    st=state
    c=US
    ea=user@example.com
  Subject:
    cn=msca-root
    ou=pki msca-root
    o=company
    l=town
    st=state
    c=US
    ea=user@example.com
  CRL Distribution Points:
    http://msca-root.example.com/CertEnroll/msca-root.crl
  Validity Date:
    start date: 22:19:29 GMT Oct 31 2002
    end   date: 22:27:27 GMT Oct 31 2017
  Subject Key Info:
    Public Key Algorithm: rsaEncryption
    RSA Public Key: (512 bit)
  Signature Algorithm: SHA1 with RSA Encryption
  Fingerprint MD5: 84E470A2 38176CB1 AA0476B9 C0B4F478
  Fingerprint SHA1: 0F57170C 654A5D7D 10973553 EFB0F94F 2FAF9837
  X509v3 extensions:
    X509v3 Key Usage: C6000000
      Digital Signature
      Non Repudiation
      Key Cert Sign
      CRL Signature
    X509v3 Subject Key ID: 37F3CC61 AF5E7C0B 434AB364 CF9FA0C1 B17C50D9
    X509v3 Basic Constraints:
        CA: TRUE
    Authority Info Access:
  Associated Trustpoints: msca-root
```

The following example shows that a self-signed certificate has been created using a user-defined trustpoint:

```
Router Self-Signed Certificate
  Status: Available
  Certificate Serial Number: 01
  Certificate Usage: General Purpose
  Issuer:
    serialNumber=C63EBBE9+ipaddress=10.3.0.18+hostname=test.company.com
  Subject:
    Name: router.company.com
    IP Address: 10.3.0.18
    Serial Number: C63EBBE9
    serialNumber=C63EBBE9+ipaddress=10.3.0.18+hostname=test.company.com
  Validity Date:
    start date: 20:51:40 GMT Nov 29 2004
    end   date: 00:00:00 GMT Jan 1 2020
  Associated Trustpoints: local
```

The following example shows that a shadow CA certificate, or rollover certificate, is available and shows its status:

```
Router# show crypto ca certificates
```

```
 Rollover Certificate

Status: Waiting for rollover
Certificate Serial Number: 3C
Certificate Usage: General Purpose
Issuer:
  cn=ezsdd
Subject:
  Name: Router.company.com
  Serial Number: 3A9BEC55
  serialNumber=3A9BEC55+hostname=Router.company.com
Validity Date:
  start date: 21:22:08 UTC Mar 17 2004
  end   date: 21:22:08 UTC Mar 17 2005
  renew date: 00:00:00 UTC Jan 1 1970
Associated Trustpoints: tti
```

Related Commands

Command	Description
crypto pki authenticate	Authenticates the CA (by obtaining the certificate of the CA).
crypto pki 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 pki certificates storage

To display the current public key infrastructure (PKI) certificate storage location, use the **show crypto pki certificates storage** command in privileged EXEC mode.

show crypto pki certificates storage

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(2)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

Use the **show crypto pki certificates storage** command to display the current PKI certificate storage location.

Examples

The following is sample output for the **show crypto pki certificates storage** command where the certificates are stored in the certs subdirectory of disk0:

```
Router# show crypto pki certificates storage

Certificates will be stored in disk0:/certs/
```

Related Commands

Command	Description
crypto pki certificate storage	Specifies local storage device for PKI certificates.

show crypto pki counters

To display the public key infrastructure (PKI) counters that are configured on the router, use the **show crypto pki counters** command in privileged EXEC mode.

show crypto pki counters

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(13)T	This command was introduced.

Examples

The following example shows the listing of all PKI counters that are configured in a router:

```
Router# show crypto pki counters

PKI Sessions Started: 5
PKI Sessions Ended: 5
PKI Sessions Active: 0
Successful Validations: 1
Failed Validations: 4
Bypassed Validations: 0
Pending Validations: 0
CRLs checked: 3
CRL - fetch attempts: 2
CRL - failed attempts: 0
AAA authorizations: 0
```

Table 120 describes the significant fields shown in the display.

Table 120 show crypto pki counters Field Descriptions

Field	Description
PKI Sessions Started	Number of PKI sessions that are started in a router.
PKI Sessions Ended	Number of PKI sessions that are ended in a router.
PKI Sessions Active	Number of PKI sessions that are actively running in a router.
Successful Validations	Number of successful PKI counter validations in a router.
Failed Validations	Number of failed PKI counter validations in a router.
Bypassed Validations	Number of validations that were bypassed during a PKI counter validation in a router.
Pending Validations	Number of pending PKI counter validations in a router.
CRLs checked	Number of certificate revocation lists (CRLs) that are checked in a PKI session.
CRL - fetch attempts	Number of times a CRL is queried and fetched.

Table 120 show crypto pki counters Field Descriptions

Field	Description
CRL - failed attempts	Number of times failed in querying and fetching a CRL.
AAA authorizations	Number of authentication, authorization, and accounting (AAA) authorizations that were used to create named methods lists in a PKI session.

Related Commands

Command	Description
show crypto pki certificates	Displays information about the certification authority certificate and any RA certificates.
show crypto pki crls	Displays the current CRL on the router.
show crypto pki server	Displays the current state and configuration of the certificate server.
show crypto pki timers	Displays the status of the managed timers that are maintained by Cisco IOS for PKI.
show crypto pki token	Displays the Cisco IOS PKI tokens that are configured on the router.
show crypto pki trustpoints	Displays the Cisco IOS PKI trustpoints that are configured in the router.

show crypto pki crls

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

show crypto pki crls

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.1	The **show crypto ca crls** command was introduced.
12.3(7)T	This command replaced the **show crypto ca crls** command.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.(33)SXH.
12.4(20)T	The output of this command was updated to include information on the CRL cache size if set by the **crypto pki crl cache** command.
Cisco IOS XE Release 2.4	This command was implemented on the Cisco ASR 1000 series routers.

Examples

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

```
Router# show crypto pki crls

          CRL Issuer Name:
              OU = vpn, O = company, 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 = vpn, O = company, C = us
```

The following is sample output of the **show crypto pki crls** command with the maximum CRL cache size set to 2048 bytes:

```
Router# show crypto pki crls

     CRL Issuer Name:
           cn=ioscs,l=Anytown,c=US
           LastUpdate: 02:53:41 GMT Mar 6 2007
           NextUpdate: 02:53:41 GMT Mar 13 2007
           Retrieved from CRL Distribution Point:
                ** CDP Not Published - Retrieved via SCEP
     CRL DER is 475 bytes
     CRL is stored in parsed CRL cache
     Parsed CRL cache current size is 1705 bytes
     Parsed CRL cache maximum size is 2048 bytes
```

Related Commands

Command	Description
crypto pki crl cache	Sets the maximum amount of volatile memory used to cache CRLs.
crypto pki crl request	Requests that a new CRL be obtained immediately from the CA.

show crypto pki server

To display the current state and configuration of the certificate server, use the **show crypto pki server** command in privileged EXEC mode.

show crypto pki server [*cs-label*]

Syntax Description

cs-label	(Optional) Name of the certificate server. The name must match the name specified through the **crypto pki server** command.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.4(2)T	The command output was modified to include shadow, or rollover, public key infrastructure (PKI) certificate information.
15.0(1)M	The command output was modified. • To include whether the server is configured for redundancy and whether its state is active or standby or simplex (active, but standby is not up). • To show the high availability (HA) status while the Hot Standby Router Protocol (HSRP) is coming up.

Usage Guidelines

At startup, the certificate server must check the current configuration before issuing any certificates. As it starts up, the certificate server transitions through the states defined in Table 121. Use the **show crypto pki server** command to display the state of the certificate server.

Table 121 Certificate Server Startup State Descriptions

Certificate Server State	Description
configured	The server is available and has generated the certificate server certificates.
storage configuration incomplete	The server is verifying that the configured storage location is available.
waiting for HTTP server	The server is verifying that the HTTP server is running.
waiting for time setting	The server is verifying that the time has been set.

Examples

The following is sample output from the **show crypto pki server** command:

```
Router# show crypto pki server

Certificate Server status: disabled, storage configuration incomplete
    Granting mode is: manual
    Last certificate issued serial number: 0
    CA certificate expiration timer: 21:29:38 GMT Jun 5 2006
    CRL NextUpdate timer: 21:31:39 GMT Jun 6 2003
    Current storage dir: ftp://myftpserver
    Database Level: Minimum - no cert data written to storage
```

Table 122 describes the significant fields shown in the display.

Table 122 show crypto pki server Field Descriptions

Field	Description
Granting mode is	Specifies whether certificate enrollment requests should be granted manually (which is the default) or automatic (through the **grant automatic** command). **Note** The **grant automatic** command should be used *only* when testing and building simple networks. This command *must* be disabled before the network is accessible by the Internet.
Last certificate issued serial number	The serial number of the latest certificate. (To specify the distinguished name (DN) as the certification authority (CA) issuer name, use the **issuer-name** command.)
CA certificate expiration timer	The expiration date for the CA certificate. (To specify the expiration date, use the **lifetime** command.)
CRL NextUpdate timer	The next time the certificate revocation list (CRL) will be updated. (To specify the CRL lifetime, in hours, use the **lifetime crl** command.)
Current storage dir	The location where all database entries for the certificate server will be written out. (To specify a location, use the **database url** command.)
Database Level	The type of data that is stored in the certificate enrollment database—Minumum, names, or complete. (To specify the data type to be stored, use **database level** command.)

The following is sample output from the **show crypto pki server** command when redundancy is configured and its state is simplex:

```
Router# show crypto pki server cert1

Certificate Server cert1:
    Status: disabled
    State: disabled
    Server's configuration is unlocked  (enter "no shut" to lock it)
    Issuer name: CN=cert1
    CA cert fingerprint: -Not found-
    Granting mode is: manual
    Last certificate issued serial number (hex): 0
    CA certificate expiration timer: 00:00:00 UTC Jan 1 1970
    CRL not present.
```

```
    Current primary storage dir: nvram:
    Database Level: Minimum - no cert data written to storage
    Redundancy configured.  Simplex mode.
```

The following is sample output from the **show crypto pki server** command when redundancy is configured and its state is active:

```
Certificate Server HA:
    Status: enabled
    State: enabled
    Server's configuration is locked  (enter "shut" to unlock it)
    Issuer name: CN=ioscs,L=Santa Cruz,C=US
    CA cert fingerprint: 42308002 188180FC 9265946F FDC68A52
    Granting mode is: auto
    Last certificate issued serial number (hex): 2
    CA certificate expiration timer: 20:22:55 PST Apr 26 2013
    CRL NextUpdate timer: 20:27:46 PST May 11 2010
    Current primary storage dir: nvram:
    Database Level: Complete - all issued certs written as <serialnum>.cer
    Redundancy configured.  This is active.
```

The following is sample output from the **show crypto pki server** command when redundancy is configured and its state is standby:

```
Certificate Server HA:
    Status: enabled
    State: enabled
    Server's configuration is locked  (enter "shut" to unlock it)
    Issuer name: CN=ioscs,L=Santa Cruz,C=US
    CA cert fingerprint: 42308002 188180FC 9265946F FDC68A52
    Granting mode is: auto
    Last certificate issued serial number (hex): 2
    CA certificate expiration timer: 20:22:55 PST Apr 26 2013
    CRL NextUpdate timer: 20:27:46 PST May 11 2010
    Current primary storage dir: nvram:
    Database Level: Complete - all issued certs written as <serialnum>.cer
    Redundancy configured.  This is standby.
```

The following example shows that the certificate server MyCS has rollover configured. Rollover has not yet occurred. The rollover status “pending” and rollover CA certificate timer show when the rollover timer will be triggered. When this timer is triggered, the shadow certificate will become the active certificate and the previously active certificate will be deleted.

```
Router# show crypto pki server

Certificate Server routercs:
   Status: enabled, configured
   Issuer name: CN=walnutcs
   CA cert fingerprint: 800F5944 74337E5B C2DF6C52 9A7B1BDB
   Granting mode is: auto
   Last certificate issued serial number: 0x6
   CA certificate expiration timer: 22:10:29 GMT Jan 29 2007
   CRL NextUpdate timer: 21:50:56 GMT Mar 5 2004
   Current storage dir: nvram:
   Database Level: Minimum - no cert data written to storage

    Rollover status: pending
    Rollover CA certificate timer: 20:34:23 GMT Jan 8 2005
```

The following example shows that the certificate server MyCS has rollover configured. The rollover time has occurred and the rollover certificate is available. The status shows the rollover certificate fingerprint and rollover CA certificate expiration timer information.

```
Router# show crypto pki server

Certificate Server routercs:
   Status: enabled, configured
   Issuer name: CN=walnutcs
   CA cert fingerprint: 800F5944 74337E5B C2DF6C52 9A7B1BDB
   Granting mode is: auto
   Last certificate issued serial number: 0x7
   CA certificate expiration timer: 22:10:29 GMT Jan 29 2007
   CRL NextUpdate timer: 21:50:56 GMT Mar 5 2004
   Current storage dir: nvram:
   Database Level: Minimum - no cert data written to storage

    Rollover status: available for rollover
    Rollover CA cert fingerprint: 6AAF5944 74227A5B 23DF3E52 9A7F1FEF
    Rollover CA certificate expiration timer: 22:10:29 GMT Jan 29 2017
```

The following example shows a certificate server (CS) that has been prevented from entering rollover state because the Cisco IOS configuration cannot be saved.

```
Router# show crypto pki server

Certificate Server routercs:
   Status: enabled, configured
   Issuer name: CN=walnutcs
   CA cert fingerprint: 800F5944 74337E5B C2DF6C52 9A7B1BDB
   Granting mode is: auto
   Last certificate issued serial number: 0x7
   CA certificate expiration timer: 22:10:29 GMT Jan 29 2007
   CRL NextUpdate timer: 21:50:56 GMT Mar 5 2004
   Current storage dir: nvram:
   Database Level: Minimum - no cert data written to storage

    Rollover status: disabled, unable to save configuration
    Rollover CA cert fingerprint: 6AAF5944 74227A5B 23DF3E52 9A7F1FEF
    Rollover CA certificate expiration timer: 22:10:29 GMT Jan 29 2017
```

Related Commands

Command	Description
crypto pki server	Enables a Cisco IOS certificate server and enter certificate server configuration mode.

show crypto pki server certificates

To display certificate information for all certificates of the specified certificate server, use the **show crypto pki server certificates** command in privileged EXEC mode.

show crypto pki server *cs-label* **certificates** [*start-number* [*end-number*]] [**expired**]

Syntax Description

cs-label	Name of the certificate server. The name must match the name specified via the **crypto pki server** command.
start-number	(Optional) The beginning of the certificate serial number range to display. If only the starting certificate serial number is indicated, information for only the designated certificate is shown if available.
end-number	(Optional) The end of the certificate serial number range to display.
expired	(Optional) Displays the expired certificates.

Command Default

Certificate information is shown for all serial numbers for the specified certificate server, from the first serial number in the certificate database to the last serial number in the certificate database.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines

This command displays available information on each certificate for the specified certificate server. If the certificate information is not available, the output displayed reads as "<cert not available>". If the certificate information is incomplete, or if it has been corrupted, the output displayed reads as "<certificate incomplete or corrupted>".

You may display information on all the certificates in the certificate database, one certificate in the certificate database, or a range of certificates in the certificate database by setting the *start-number* and *end-number* arguments.

Examples

The following example shows the listing of all certificates in the certificate database for the certificate server "mycs":

```
Router# show crypto pki server mycs certificates

Serial   Issued date               Expire date               Subject Name
1        02:09:09 PST Jan 22 2007  02:09:09 PST Jan 21 2010  cn=company
2        02:57:59 PST Jan 22 2007  02:57:59 PST Jan 22 2008  hostname=client.example.com
3        03:00:12 PST Jan 22 2007  03:00:12 PST Jan 22 2008  hostname=client.example.com
4        19:53:07 PST Jan 18 2007  19:53:07 PST Jan 19 2007  hostname=client.example.com
5        <cert not available>
6        <cert not available>
7        <cert not available>
```

```
8        02:57:59 PST Jan 22 2007  02:57:59 PST Jan 22 2008  hostname=client.example.com
9        <Certificate incomplete or corrupted>
A        <cert not available>
B        <cert not available>
```

The following example shows the information for certificate serial number 3 in the certificate database for the certificate server “mycs”:

```
Router# show crypto pki server mycs certificates start 3

Serial   Issued date               Expire date               Subject Name
3        03:00:12 PST Jan 22 2007  03:00:12 PST Jan 22 2008  hostname=client.example.com
```

The following example shows the information for certificate serial number 3 through certificate serial number 7 in the certificate database for the certificate server “mycs”:

```
Router# show crypto pki server mycs certificates start 3 end 7

show crypto pki server mycs certificates
Serial   Issued date               Expire date               Subject Name
3        03:00:12 PST Jan 22 2007  03:00:12 PST Jan 22 2008  hostname=client.example.com
4        19:53:07 PST Jan 18 2007  19:53:07 PST Jan 19 2007  hostname=client.example.com
5        <cert not available>
6        <cert not available>
7        <cert not available>
```

Related Commands

Command	Description
crypto pki server	Enables a Cisco IOS certificate server and enters certificate server configuration mode.
show crypto pki server	Displays the current state and configuration of the certificate server.
show crypto pki server crl	Displays the current status of the CRL.

show crypto pki server crl

To display information regarding the status of the current certificate revocation list (CRL), use the **show crypto pki server crl** command in privileged EXEC mode.

show crypto pki server *cs-label* **crl**

Syntax Description

cs-label	Name of the certificate server. The name must match the name specified via the **crypto pki server** command.

Command Defaults

None.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines

CRLs are issued once every specified time period via the **lifetime crl** command. It is the responsibility of the network administrator to ensure that the CRL is available from the location that is specified via the **cdp-url** command. To access information, such as the lifetime and location of the CRL, use the **show crypto pki server crl** command.

Examples

The following example shows how to access CRL information for the certificate server “mycs”:

```
Router# show crypto pki server mycs crl
```

Related Commands

Command	Description
cdp-url	Specifies a CDP to be used in certificates that are issued by the certificate server.
crypto pki server	Enables a Cisco IOS certificate server and enter certificate server configuration mode.
lifetime crl	Defines the lifetime of the CRL that is used by the certificate server.

show crypto pki server requests

To display all outstanding certificate enrollment requests, use the **show crypto pki server requests** command in privileged EXEC mode.

show crypto pki server *cs-label* **requests**

Syntax Description

cs-label	Name of the certificate server. The name must match the name specified via the **crypto pki server** command.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines

A certificate enrollment request functions as follows:

- The certificate server receives the enrollment request from an end user, and the following actions occur:
  - A request entry is created in the enrollment request database with the initial state. (See the **show pki server** command for a complete list of certificate enrollment request states.)
  - The certificate server refers to the command-line interface (CLI) configuration (or the default behavior any time a parameter is not specified) to determine the authorization of the request. Thereafter, the state of the enrollment request is updated in the enrollment request database.
- At each Simple Certificate Enrollment Protocol (SCEP) query for a response, the certificate server examines the current request and performs one of the following actions:
  - Responds to the end user with a “pending” or “denied” state.
  - Forwards to the request to the certification authority (CA) core, where it will generate and sign the appropriate certificate, store the certificate in the enrollment request database, and return the request to the built-in certificate server SCEP server, who will reply to the end user with the certificate on the next SCEP request.

If the connection of the client has closed, the certificate server will wait for the client user to request another certificate.

All enrollment requests transitions through the certificate enrollment states that are defined in Table 123.

Table 123 Certificate Enrollment Request State Descriptions

Certificate Enrollment State	Description
authorized	The certificate server has authorized the request.
denied	The certificate server has denied the request for policy reasons.
granted	The CA core has generated the appropriate certificate for the certificate request.
initial	The request has been created by the SCEP server.
malformed	The certificate server has determined that the request is invalid for cryptographic reasons.
pending	The enrollment request must be manually accepted by the network administrator.

Examples

The following example shows output for the certificate server "certsrv1," which has a pending certificate enrollment request:

```
Router# show crypto pki server certsrv1 requests

   Enrollment Request Database:
   ReqID  State      Fingerprint                       SubjectName
   --------------------------------------------------------------
   1      pending    0A71820219260E526D250ECC59857C2D serialNumber=2326115A+hostname=831.
```

The following example shows the output for shadow public key infrastructure (PKI) certificate info requests:

```
Router# show crypto pki server mycs requests

Enrollment Request Database:

RA certificate requests:

  ReqID  State      Fingerprint                       SubjectName

--------------------------------------------------------------
RA rollover certificate requests:

  ReqID  State      Fingerprint                       SubjectName

  --------------------------------------------------------------

Router certificates requests:

  ReqID  State      Fingerprint                       SubjectName

--------------------------------------------------------------

1      pending    A426AF07FE3A4BB69062E0E47198E5BF hostname=client

  Router rollover certificates requests:

  ReqID  State      Fingerprint                       SubjectName

  --------------------------------------------------------------

  2      pending    B69062E0E47198E5BFA426AF07FE3A4B hostname=client
```

Related Commands

Command	Description
crypto pki server	Enables a Cisco IOS certificate server and enters PKI configuration mode.

show crypto pki timers

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

show crypto pki timers

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(8)T	The **show crypto ca timers** command was introduced.
12.3(7)T	This command replaced the **show crypto ca timers** command.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.

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 pki timers** command:

```
Router# show crypto pki 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 pki trustpoint	Declares the CA that your router should use.

show crypto pki token

To display the Cisco IOS public key infrastructure (PKI) tokens that are configured on the router, use the **show crypto pki token** command in privileged EXEC mode.

show crypto pki token [*name*]

Syntax Description

name	(Optional) Specifies the name of the token.

Command Default

If the *name* argument is not specified, command output is displayed for all PKI tokens.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(15)T	This command was introduced.

Examples

The following is sample output from the **show crypto pki token** command:

```
Router# show crypto pki token

Configuration for token usbtoken0:
Automatic login enabled.
Removal timeout 60 seconds

Configuration for token default:
Secondary Config file "BIFT.CFG"
```

Table 124 describes the significant fields shown in the display.

Table 124 show crypto pki token Field Descriptions

Field	Description
Automatic login enabled	Indicates that the crypto PKI token is configured to log in automatically.
Removal timeout 60 seconds	Indicates that the router waits for 60 seconds before removing the Rivest, Shamir, and Adelman (RSA) keys that are stored in the eToken.
Secondary Config file	Indicates that the specified file will be merged with the running configuration after the eToken is logged into the router.

Related Commands

Command	Description
crypto pki token removal timeout	Sets the time interval that the router waits before removing the RSA keys that are stored in the eToken.
crypto pki token secondary config	Merges a specified file with the running configuration after the eToken is logged into the router.

show crypto pki trustpoints

To display the trustpoints that are configured in the router, use the **show crypto pki trustpoints** command in privileged EXEC or user EXEC mode.

show crypto pki trustpoints [**status** | *label* [**status**]]

Syntax Description

status	(Optional) Trustpoint status.
label	(Optional) Trustpoint name.

Command Default

If the *label* argument (trustpoint name) is not specified, command output is displayed for all trustpoints.

Command Modes

Privileged EXEC (#)
User EXEC (>)

Command History

Release	Modification
12.2(8)T	The **show crypto ca trustpoints** command was introduced.
12.3(7)T	This command replaced the **show crypto ca trustpoints** command.
12.3(11)T	The **status** keyword and *label* argument were added.
12.3(14)T	The command output was modified to include persistent self-signed certificate parameters.
12.4(2)T	The command output was modified to include shadow, or rollover, public key infrastructure (PKI) certificate availability and Simple Certificate Enrollment Protocol (SCEP) capabilities.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(22)T	The command output was modified to include X.509 certificate IP address extension information.

Examples

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

```
Router# show crypto pki trustpoints

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

The following is sample output from the **show crypto pki trustpoints** command when a persistent self-signed certificate has been configured:

```
Router# show crypto pki trustpoints

Trustpoint local:
    Subject Name:
    serialNumber=C63EBBE9+ipaddress=10.3.0.18+hostname=test.company.com
          Serial Number: 01
    Persistent self-signed certificate trust point
```

The following output shows that a shadow PKI certificate is available and shows the SCEP capabilities:

```
Router# show crypto pki trustpoints

Trustpoint vpn:
   Subject Name:
   cn=Company SSL CA
   o=Company

   Serial Number: 0FFEBBDC1B6F6D9D0EA7875875E4C695

   Certificate configured.

   Rollover certificate configured.
   Enrollment Protocol:
   SCEPv1, PKI Rollover
```

The following output using the **status** keyword shows that the trustpoint is configured in query mode and is currently trying to query the certificates (the certificate authority (CA) certificate and the router certificate are both pending):

```
Router# show crypto pki trustpoints status

Trustpoint yni:
  Issuing CA certificate pending:
    Subject Name:
     cn=r1 Cert Manager,ou=pki,o=company.com,c=country
    Fingerprint: C21514AC 12815946 09F635ED FBB6CF31
  Router certificate pending:
    Subject Name:
     hostname=host.company.com,o=company.com
  Next query attempt:
    52 seconds
```

The following output using the **status** keyword shows that the trustpoint has been authenticated:

```
Router# show crypto pki trustpoints status

Trustpoint yni:
  Issuing CA certificate configured:
    Subject Name:
     cn=r1 Cert Manager,ou=pki,o=company.com,c=country
    Fingerprint: C21514AC 12815946 09F635ED FBB6CF31
  State:
    Keys generated ..... No
    Issuing CA authenticated ..... Yes
    Certificate request(s) ..... None
```

The following output using the **status** keyword shows that the trustpoint is enrolling and that two of the certificate requests are pending (Signature and Encryption):

```
Router# show crypto pki trustpoints status

Trustpoint yni:
  Issuing CA certificate configured:
    Subject Name:
     cn=r1 Cert Manager,ou=pki,o=company.com,c=country
    Fingerprint: C21514AC 12815946 09F635ED FBB6CF31
  Router Signature certificate pending:
    Requested Subject Name:
     hostname=host.company.com
    Request Fingerprint: FAE0D74E BB844EA1 54B26698 56AB42EC
    Enrollment polling: 1 times (9 left)
    Next poll: 32 seconds
  Router Encryption certificate pending:
    Requested Subject Name:
     hostname=host.company.com
    Request Fingerprint: F4E815DB D9D9B60F 9B5B1724 3E155DBF
    Enrollment polling: 1 times (9 left)
    Next poll: 44 seconds
  Last enrollment status: Pending
  State:
    Keys generated ..... Yes (Signature, Encryption)
    Issuing CA authenticated ..... Yes
    Certificate request(s) ..... Pending
```

The following output using the **status** keyword shows that enrollment has succeeded and that two router certificates have been granted (Signature and Encryption):

```
Router# show crypto pki trustpoints status

Trustpoint yni:
  Issuing CA certificate configured:
    Subject Name:
     cn=r1 Cert Manager,ou=pki,o=company.com,c=country
    Fingerprint: C21514AC 12815946 09F635ED FBB6CF31
  Router Signature certificate configured:
    Subject Name:
     hostname=host.company.com,o=company.com
    Fingerprint: 8A370B8B 3B6A2464 F962178E 8385E9D6
  Router Encryption certificate configured:
    Subject Name:
     hostname=host.company.com,o=company.com
    Fingerprint: 43A03218 C0AFF844 AE0C162A 690B414A
  Last enrollment status: Granted
  State:
    Keys generated ..... Yes (Signature, Encryption)
    Issuing CA authenticated ..... Yes
    Certificate request(s) ..... Yes
```

The following output using the **status** keyword shows that trustpoint enrollment has been rejected:

```
Router# show crypto pki trustpoints status

Trustpoint yni:
  Issuing CA certificate configured:
    Subject Name:
     cn=r1 Cert Manager,ou=pki,o=company.com,c=country
    Fingerprint: C21514AC 12815946 09F635ED FBB6CF31
  Last enrollment status: Rejected
  State:
    Keys generated ..... Yes (General Purpose)
```

```
    Issuing CA authenticated ....... Yes
    Certificate request(s) ..... None
```

The following output using the **status** keyword shows that enrollment has succeeded and that the router is configured for autoenrollment using a regenerated key. In addition, the running configuration has been modified so that it will not be saved automatically after autoenrollment.

```
Router# show crypto pki trustpoints status

Trustpoint yni:
  Issuing CA certificate configured:
    Subject Name:
     cn=r1 Cert Manager,ou=pki,o=company.com,c=country
    Fingerprint: C21514AC 12815946 09F635ED FBB6CF31
  Router General Purpose certificate configured:
    Subject Name:
     hostname=host.company.com,o=company.com
    Fingerprint: FC365F95 E24D4B55 81347510 10FFE331
  Last enrollment status: Granted
  Next enrollment attempt:
    01:58:25 PST Feb 14 2004
    * A new key will be generated *
    * Configuration will not be saved after enrollment *
  State:
    Keys generated ..... Yes (General Purpose)
    Issuing CA authenticated ....... Yes
    Certificate request(s) ..... Yes
```

Table 125 describes the significant fields shown in the display.

Table 125 show crypto pki trustpoints Field Descriptions

Field	Description
Trustpoint	Name of the trustpoint.
Issuing CA certificate pending	The CA certificate is being retrieved (query mode).
Issuing CA certificate [not] configured	A CA certificate is [not] configured.
Subject Name	Subject name of the indicated certificate.
Next query attempt	Time until the next query attempt (query mode).
Router certificate pending/Router [key usage] certificate pending	The trustpoint is attempting to obtain the certificate from the CA server (through query mode or enrollment).
Router [key usage] certificate configured	Certificate of the specified key usage is configured.
Requested Subject Name	Subject name used in the enrollment request (Public Key Cryptography Standards 10 [PKCS10]).
Fingerprint MD5/SHA1	Fingerprint of the indicated certificate (Message Digest 5 [MD5] or Secure Hash Algorithm 1 [SHA]1).
Request Fingerprint MD5/SHA1	Fingerprint of the PKCS10 enrollment request (MD5/SHA1).
Enrollment polling: [polled] times ([remaining] left)/Next poll: in seconds	Number of SCEP polling attempts that have been made and that remain before the router gives up/Time until the next polling attempt.
Last enrollment status: Pending/Granted/Rejected/Failed	Last enrollment attempt status (pending, granted, rejected, or failed).

Table 125 show crypto pki trustpoints Field Descriptions (continued)

Field	Description
Next enrollment attempt: *time* (Optional) A new key will be generated. (Optional) Configuration will not be saved after enrollment.	The trustpoint is configured autoenrollment and the autoenrollment will happen at *time*. (Optional) The trustpoint is configured to generate a new key when autoenrollment occurs. (Optional) The running configuration is "dirty," so the configuration will not be saved automatically after autoenrollment.
State	Current state of the trustpoint.
Keys generated	"Yes or No" and the key usage (General Purpose or Signature, Encryption).
Issuing CA authenticated	"Yes or No" if crypto CA authentication has been done successfully.
Certificate request(s)	Progress of current enrollment: "Pending," "Yes," (complete), or "None" (not in progress).

Related Commands

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

show crypto route

To display routes that are created through IPsec via Reverse Route Injection (RRI) or Easy VPN virtual tunnel interfaces (VTIs) in one table, use the **show crypto route** command in privileged EXEC mode.

show crypto route

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(15)T	This command was introduced.

Examples

The following example displays routes that were created through IPSec using RRI and VTIs:

```
Router# show crypto route

VPN Routing Table: Shows RRI and VTI created routes
Codes: RRI - Reverse-Route, VTI- Virtual Tunnel Interface
        S - Static Map ACLs

Routes created in table GLOBAL DEFAULT
192.168.6.2/255.255.255.255 [0/0] via 10.0.0.133
                                  on Virtual-Access3 RRI
10.1.1.0/255.255.255.0 [10/0] via Virtual-Access2 VTI
192.168.6.1/255.255.255.255 [0/0] via Virtual-Access2 VTI
```

The fields in the above display are self-explanatory.

Related Commands

Command	Description
reverse-route	Creates source proxy information for a crypto map entry.
set reverse-route	Defines a distance metric for each static route or tags a RRI-created route.

show crypto ruleset

To display information about crypto rules on outgoing packets, use the **show crypto ruleset** command in privileged EXEC mode.

show crypto ruleset [**detail**]

Syntax Description

detail	Displays the directional mode of the IP security (IPsec) security association (SA).

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(20)T	This command was introduced.

Examples

The following example displays information about the crypto rules on outgoing packets:

```
Router# show crypto ruleset

Ethernet0/0:
  59 ANY ANY DENY
  11 ANY/848 ANY/848 DENY
 IP ANY ANY IPSec SA Passive
 IP ANY ANY IPSec Cryptomap
```

The following output example shows the directional mode of the IPsec SA:

```
Router# show crypto ruleset detail

Ethernet0/0:
 20000001000019  59 ANY ANY DENY -> 20000001999999
 20000001000029  11 ANY/848 ANY/848 DENY -> 20000001999999
 20000001000035 IP ANY ANY IPSec SA Passive
 20000001000039 IP ANY ANY IPSec Cryptomap
```

Table 126 describes the significant fields shown in the display.

Table 126 show crypto ruleset Field Descriptions

Field	Description
59 ANY ANY DENY	• 59—Hex value of the Open Shortest Path First (OSPF) protocol. • First ANY—Any source IP address. • Second ANY—Any destination IP address. • DENY packets matching this rule will not be encrypted.
11 ANY/848 ANY/848 DENY	• 11—Hex value of the User Datagram Protocol (UDP). • First ANY/848—Any source IP address that has a source port 848. • Second ANY/848—Any destination IP address having a destination port 848. • DENY—Packets matching this rule will not be encrypted.
IP ANY ANY IPSec SA Passive	• Policy of “IP packets with any source or destination address or port” is in IPsec security association (SA) passive mode—Receives both clear and encrypted packets; sends only encrypted packets.
IP ANY ANY IPSec Cryptomap	• Policy of "IP packets with any source or destination address or port" is created by an IPsec crypto map—Receives or sends only encrypted packets.
20000001000019 59 ANY ANY DENY -> 20000001999999	• The first long digit is the priority number of the policy or rule. • The second long digit is the deny priority number of the policy or rule. **Note** These numbers are internal data values and are generally used by developers.

show crypto session

To display status information for active crypto sessions, use the **show crypto session** command in privileged EXEC mode.

show crypto session [**groups** | **interface** *type* [**brief** | **detail**] | **isakmp** [**group** *group-name* | **profile** *profile-name*] [**brief** | **detail**] | [**local** | **remote**] [*ip-address* | *ipv6-address*] [**port** *portnumber*] | [**fvrf** *fvrf-name*] [**ivrf** *ivrf-name*] [**brief** | **detail**] | **summary** *group-name* | **username** *username*]

IPsec and IKE Stateful Failover Syntax

show crypto session [**active** | **standby**]

Syntax Description

groups	(Optional) Displays crypto session group usage for all groups.
interface *type*	(Optional) Displays crypto sessions on the connected interface. • The *type* value is the type of interface connection.
brief	(Optional) Provides brief information about the session, such as the peer IP address, interface, username, group name/phase1 ID, length of session uptime, and current session status (up/down).
detail	(Optional) Provides more detailed information about the session, such as the capability of the Internet Key Exchange (IKE) security association (SA), connection ID, remaining lifetime of the IKE SA, inbound or outbound encrypted or decrypted packet number of the IP security (IPsec) flow, dropped packet number, and kilobyte-per-second lifetime of the IPsec SA.
isakmp group *group-name*	(Optional) Displays crypto sessions using the Internet Security Association and Key Management Protocol (ISAKMP) group. • The *group-name* value is the name of the group.
profile *profile-name*	(Optional) Displays crypto sessions using the ISAKMP profile. • The *profile-name* value is the name of the profile.
local	(Optional) Displays status information about crypto sessions of a local crypto endpoint.
remote	(Optional) Displays status information about crypto sessions of a remote session.
ip-address	IP address of the local or remote crypto endpoint.
ipv6-address	IPv6 address of the local or remote crypto endpoint.
port *portnumber*	(Optional) Port of the local crypto endpoint. • *The portnumber* value can be 1 through 65535. The default value is 500.
fvrf *fvrf-name*	(Optional) Displays status information about the front door virtual routing and forwarding (FVRF) session. • The *fvrf-name* value is the name of the FVRF session.
ivrf *ivrf-name*	(Optional) Displays status information about the inside VRF (IVRF) session. • The *ivrf-name* value is the name of the IVRF session.

summary *group-name*	(Optional) Displays a list of crypto session groups and associated group members.
username *username*	(Optional) Displays the crypto session for the specified extended authentication (XAUTH), public key infrastructure (PKI), or authentication, authorization, and accounting (AAA) username.
active	(Optional) Displays all crypto sessions in the active state.
standby	(Optional) Displays all crypto sessions that are in the standby state.

Command Default

All existing sessions will be displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
12.3(11)T	This command was modified. The **active** and **standby** keywords were added.
12.4(4)T	This command was modified. IPv6 address information was added to the command output.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.(33)SRA.
12.4(11)T	This command was modified. The **brief**, **groups**, **interface** *type***, isakmp group** *group-name***, isakmp profile** *profile-name*, **summary**, and **username** *username* keywords and arguments were added. The **show crypto session** output was updated to include username, ISAKMP profile, ISAKMP group, assigned address, and session uptime.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

This command lists all the active Virtual Private Network (VPN) sessions and the IKE and IPsec SAs for each VPN session. The listing will include the following information:

- Interface
- IKE peer description, if available
- IKE SAs that are associated with the peer by which the IPsec SAs are created
- IPsec SAs serving the flows of a session

Multiple IKE or IPsec SAs may be established for the same peer (for the same session), in which case IKE peer descriptions will be repeated with different values for the IKE SAs that are associated with the peer and for the IPsec SAs that are serving the flows of the session.

IPv6 does not support the **fvfr** and **ivrf** keywords and the *vrf-name* argument.

Examples

The following example shows the status information for all active crypto sessions:

```
Router# show crypto session

Crypto session current status

Interface: Virtual-Access2
Username: cisco
Profile: prof
Group: easy
Assigned address: 10.3.3.4
Session status: UP-ACTIVE
Peer: 10.1.1.2 port 500
  IKE SA: local 10.1.1.1/500 remote 10.1.1.2/500 Active
  IKE SA: local 10.1.1.1/500 remote 10.1.1.2/500 Inactive
  IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 host 3.3.3.4
        Active SAs: 2, origin: crypto map
```

The following is sample output from the **show crypto session brief** command:

```
Router# show crypto session brief

Status: A- Active, U - Up, D - Down, I - Idle, S - Standby, N - Negotiating
        K - No IKE
ivrf = (none)
           Peer         I/F     Username     Group/Phase1_id    Uptime      Status
           10.1.1.2     Vi2     cisco        easy               00:50:30    UA
```

The following is sample output from the **show crypto session detail** command:

```
Router# show crypto session detail

Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, X - IKE Extended Authentication

Interface: Virtual-Access2
Username: cisco
Profile: prof
Group: easy
Assigned address: 10.3.3.4
Uptime: 00:49:33
Session status: UP-ACTIVE
Peer: 10.1.1.2 port 500 fvrf: (none) ivrf: (none)
Phase1_id: easy
Desc: (none)
IKE SA: local 10.1.1.1/500 remote 10.1.1.2/500 Active
Capabilities:CX connid:1002 lifetime:23:10:15
IPSEC FLOW: permit ip 10.0.0.0/0.0.0.0 host 10.3.3.4
Active SAs: 2, origin: crypto map
Inbound: #pkts dec'ed 0 drop 0 life (KB/Sec) 4425776/626
Outbound: #pkts enc'ed 0 drop 0 life (KB/Sec) 4425776/626
```

Table 127 describes the significant fields shown in the display.

Table 127 show crypto session Field Descriptions

Field	Description
Interface	Interface to which the crypto session is related.
Session status	Current status of the crypto (VPN) sessions. See Table 128 for explanations of the status of the IKE SA, IPsec SA, and tunnel as shown in the display.
IKE SA	Information about the IKE SA, such as local and remote address and port, SA status, SA capabilities, crypto engine connection ID, and remaining lifetime of the IKE SA.
IPSEC FLOW	A snapshot of information about the IPsec-protected traffic flow, such as the status of the flow (for example, permit IP host 10.1.1.5 host 10.1.2.5), the number of IPsec SAs, the origin of the SA, such as manually entered, dynamic, or static crypto maps, number of encrypted or decrypted packets or dropped packets, and the IPsec SA remaining lifetime in kilobytes per second.

Table 128 provides an explanation of the current status of the VPN sessions shown in the display.

Table 128 Current Status of the VPN Sessions

IKE SA	IPsec SA	Tunnel Status
Exist, active	Exist (flow exists)	UP-ACTIVE
Exist, active	None (flow exists)	UP-IDLE
Exist, active	None (no flow)	UP-IDLE
Exist, inactive	Exist (flow exists)	UP-NO-IKE
Exist, inactive	None (flow exists)	DOWN-NEGOTIATING
Exist, inactive	None (no flow)	DOWN-NEGOTIATING
None	Exist (flow exists)	UP-NO-IKE
None	None (flow exists)	DOWN
None	None (no flow)	DOWN

Note IPsec flow may not exist if a dynamic crypto map is being used.

The following sample output shows all crypto sessions that are in the standby state:

```
Router# show crypto session standby

Crypto session current status

Interface: Ethernet0/0
Session status: UP-STANDBY
Peer: 10.165.200.225 port 500
  IKE SA: local 10.165.201.3/500 remote 10.165.200.225/500 Active
  IKE SA: local 10.165.201.3/500 remote 10.165.200.225/500 Active
```

```
IPSEC FLOW: permit ip host 192.168.0.1 host 172.16.0.1
      Active SAs: 4, origin: crypto map
```

Related Commands

Command	Description
clear crypto session	Deletes crypto sessions (IPsec and IKE SAs).
description	Adds a description for an IKE peer.
show crypto isakmp peer	Displays peer descriptions.

show crypto session group

To display groups that are currently active on the Virtual Private Network (VPN) device, use the **show crypto session group** command in privileged EXEC mode.

show crypto session group

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS 12.2SX family of releases. Support in a specific 12.2SX release is dependent on your feature set, platform, and platform hardware.

Usage Guidelines

If the **crypto isakmp client configuration group** command and **max-users** keyword have not been enabled in any VPN group profile, this command will yield a blank result.

Examples

The following example shows that at least one session is active for the group Connections:

```
Router# show crypto session group

 Group: Connections
 cisco: 1
```

Related Commands

Command	Description
crypto isakmp client configuration group	Specifies to which group a policy profile will be defined.
show crypto session summary	Displays groups that are currently active on the VPN device and the users that are connected for each of those groups.

show crypto session summary

To display groups that are currently active on the Virtual Private Network (VPN) device and the users that are connected for each of those groups, use the **show crypto session summary** command in privileged EXEC mode.

show crypto session summary

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS 12.2SX family of releases. Support in a specific 12.2SX release is dependent on your feature set, platform, and platform hardware.

Usage Guidelines

If the **crypto isakmp client configuration group** command and **max-users** keyword are not enabled in any VPN group profile and the **crypto isakmp client configuration group** command and **max-logins** keyword are not enabled, this command will yield a blank result.

Examples

The following example shows that the group “cisco” is active and that it has one user connected, green, who is connected one time. The number in parentheses (1) is the number of simultaneous logins for that user.

```
Router# show crypto session summary

 Group cisco has 1 connections
  User (Logins)
  green (1)
```

Related Commands

Command	Description
crypto isakmp client configuration group	Specifies to which group a policy profile will be defined.
show crypto session group	Displays groups that are currently active on the VPN device.

show crypto socket

To list crypto sockets, use the **show crypto socket** command in privileged EXEC mode.

show crypto socket

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(11)T	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.4(5)	The Flags field was added to command output.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.(33)SRA.

Usage Guidelines

Use this command to list crypto sockets and the state of the sockets.

Examples

The following sample output shows the number of crypto socket connections (2) and their state:

```
Router# show crypto socket

Number of Crypto Socket connections 2

   Tu0 Peers (local/remote): 192.168.2.2/192.168.1.1
       Local Ident  (addr/mask/port/prot): (192.168.2.2/255.255.255.255/0/47)
       Remote Ident (addr/mask/port/prot): (192.168.1.1/255.255.255.255/0/47)
       Flags: shared
       Socket State: Open
       Client: "TUNNEL SEC" (Client State: Active)
   Tu1 Peers (local/remote): 192.168.2.2/192.168.1.3
       Local Ident  (addr/mask/port/prot): (192.168.2.2/255.255.255.255/0/47)
       Remote Ident (addr/mask/port/prot): (192.168.1.3/255.255.255.255/0/47)
       Flags: shared
       Socket State: Open
       Client: "TUNNEL SEC" (Client State: Active)

Crypto Sockets in Listen state:
Client: "TUNNEL SEC" Profile: "dmvpn-profile" Map-name: "dmvpn-profile-head-2"
```

Table 129 describes the significant fields in the display.

Table 129 show crypto socket Field Descriptions

Field	Description
Number of Crypto Socket connections	Number of crypto sockets in the system.
Socket State	This state can be Open, which means that active IPSec security associations (SAs) exist, or it can be Closed, which means that no active IPSec SAs exist.
Client	Application name and its state.
Flags	If this field says “shared,” the socket is shared with more than one tunnel interface.
Crypto Sockets in Listen state	Name of the crypto IPSec profile.

show crypto tech-support

To display the crypto technical support information, use the **show crypto tech-support** command in privileged EXEC mode.

show crypto tech-support [**peer** *ip-address* | **vrf** *vrf-name*]

Syntax Description

peer	(Optional) Displays the crypto technical support information related to a peer.
ip-address	(Optional) The peer IPv4 address.
vrf	(Optional) Displays the crypto technical support information related to VPN routing or forwarding (VRF).
vrf-name	(Optional) The VRF name.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(22)T	This command was introduced.

Usage Guidelines

Use the optional keywords and arguments to display the specific crypto technical support information.

Examples

The following is sample output from the **show crypto tech-support** command. The fields are self-explanatory.

```
Router# show crypto tech-support

------------------ show crypto session remote 1.0.1.2 detail ------------------

------------------ show crypto ipsec sa peer 1.0.1.2 detail ------------------

------------------ show crypto isakmp sa peer 1.0.1.2 detail ------------------

IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status

------------------ show crypto isakmp peers 1.0.1.2  ------------------

------------------ show crypto ruleset detail ------------------

------------------ show processes memory | include  Crypto IKMP ----------------

 240   0       7112        252      20064           0           0 Crypto IKMP

------------------ show processes cpu |  include Crypto IKMP ------------------

 240           0         3           0  0.00%  0.00%  0.00%   0 Crypto IKMP

------------------ show crypto eli ------------------
```

```
Hardware Encryption : ACTIVE
 Number of hardware crypto engines = 1

 CryptoEngine Onboard VPN details: state = Active
 Capability      : IPPCP, DES, 3DES, AES, IPv6, FAILCLOSE

 IPSec-Session :     0 active,  1400 max, 0 failed


------------------ show cry engine accelerator statistic ------------------
Device:   Onboard VPN
Location: Onboard: 0
        :Statistics for encryption device since the last clear
         of counters 1818819 seconds ago
                      0 packets in                          0 packets out
                      0 bytes in                            0 bytes out
                      0 paks/sec in                         0 paks/sec out
                      0 Kbits/sec in                        0 Kbits/sec out
                      0 packets decrypted                   0 packets encrypte
                      0 bytes before decrypt                0 bytes encrypted
                      0 bytes decrypted                     0 bytes after encr
                      0 packets decompressed                0 packets compress
                      0 bytes before decomp                 0 bytes before com
                      0 bytes after decomp                  0 bytes after comp
                      0 packets bypass decompr              0 packets bypass cs
                      0 bytes bypass decompres              0 bytes bypass comi
                      0 packets not decompress              0 packets not compd
                      0 bytes not decompressed              0 bytes not compre
                    1.0:1 compression ratio               1.0:1 overall
                  Last 5 minutes:
                      0 packets in                          0 packets out
```

show crypto vlan

To display the VPN running state for an IPSec VPN SPA, use the **show crypto vlan** command in privileged EXEC mode.

show crypto vlan

Defaults

No default behavior or values.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(18)SXE2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

When you show the configuration, the crypto engine subslot configuration state is expressed in the context of the associated interface VLAN. The interface VLAN is also shown as having been added to the appropriate inside trunk port. This is the case even if the configuration was loaded from a legacy (pre-crypto engine subslot) configuration file, or if VLANs were manually added instead of being added through the **crypto engine subslot** command.

Examples

In the following example, the interface VLAN belongs to the IPSec VPN SPA inside port:

```
Router# show crypto vlan
  Interface VLAN 2 on IPSec Service Module port 7/1/1 connected to Fa8/3
```

In the following example, VLAN 2 is the interface VLAN and VLAN 2022 is the hidden VLAN:

```
Router# show crypto vlan
Interface VLAN 2 on IPSec Service Module port 3/1/1 connected to VLAN 2022 with crypto map
set coral2
```

In the following example, either the interface VLAN is missing on the IPSec VPN SPA inside port, the IPSec VPN SPA is removed from the chassis, or the IPSec VPN SPA was moved to a different subslot:

```
Router# show crypto vlan
  Interface VLAN 2 connected to VLAN 3 (no IPSec Service Module attached)
```

Related Commandss

Command	Description
crypto connect vlan	Creates an interface VLAN for an IPSec VPN SPA and enters crypto-connect mode.
crypto engine subslot	Assigns an interface VLAN that requires encryption to the IPSec VPN SPA.