

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

```

show crypto isakmp policy

```

    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 65](#) describes the significant fields shown in the display.

Table 65 *show crypto isakmp profile* Field Descriptions

| Field | Description |
|----------------|-----------------------------|
| ISAKMP PROFILE | Name of the ISAKMP profile. |

Table 65 *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 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. |
| <i>map-name</i> | | Name of the specified crypto map. |
| interface <i>interface</i> | (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 <i>map-tag</i> 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 66](#) describes the significant fields shown in the display.

Table 66 *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 66 *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.

■ show crypto map (IPsec)

```

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 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 <i>type</i> | (Optional) Displays crypto sessions on the connected interface. <ul style="list-style-type: none"> The <i>type</i> 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/phase 1 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 IPsec flow, dropped packet number, and kilobyte-per-second lifetime of the IPsec SA. |
| isakmp group <i>group-name</i> | (Optional) Displays crypto sessions using the Internet Security Association and Key Management Protocol (ISAKMP) group. <ul style="list-style-type: none"> The <i>group-name</i> value is the name of the group. |
| profile <i>profile-name</i> | (Optional) Displays crypto sessions using the ISAKMP profile. <ul style="list-style-type: none"> The <i>profile-name</i> 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. |
| <i>ip-address</i> | IP address of the local or remote crypto endpoint. |
| <i>ipv6-address</i> | IPv6 address of the local or remote crypto endpoint. |
| port <i>portnumber</i> | (Optional) Port of the local crypto endpoint. <ul style="list-style-type: none"> The <i>portnumber</i> value can be 1 through 65535. The default value is 500. |
| fvrf <i>fvrf-name</i> | (Optional) Displays status information about the front door virtual routing and forwarding (FVRF) session. <ul style="list-style-type: none"> The <i>fvrf-name</i> value is the name of the FVRF session. |
| ivrf <i>ivrf-name</i> | (Optional) Displays status information about the inside VRF (IVRF) session. <ul style="list-style-type: none"> The <i>ivrf-name</i> value is the name of the IVRF session. |

| | |
|----------------------------------|---|
| summary <i>group-name</i> | (Optional) Displays a list of crypto session groups and associated group members. |
| username <i>username</i> | (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 (#)

| 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 <i>interface-type</i> , isakmp group <i>group-name</i> , isakmp profile <i>profile-name</i> , summary , and username <i>username</i> 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 of 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 **fvrf** 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 67 describes the significant fields shown in the display.

Table 67 *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 68 for explanations of the status of the IKE SA, IPsec SA, and tunnel as shown in the display. |
| IKE SA | Information is provided 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 map, number of encrypted or decrypted packets or dropped packets, and the IPsec SA remaining lifetime in kilobytes per second. |

Table 68 provides an explanation of the current status of the VPN sessions shown in the display.

Table 68 *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 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. |
| | Cisco IOS XE Release 2.1 | This command was introduced on Cisco ASR 1000 Series Routers. |

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 its 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"
```

Significant fields are described in [Table 69](#).

Table 69 *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. |
| Crypto Sockets in Listen state | Name of the crypto IPsec profile. |
| Flags | If this field says "shared," the socket is shared with more than one tunnel interface. |

show dial-peer voice

To display information for voice dial peers, use the **show dial-peer voice** command in user EXEC or privileged EXEC mode.

show dial-peer voice [*number* | **busy-trigger-counter** | **summary** | **voip system**]

Syntax Description

| | |
|-----------------------------|---|
| <i>number</i> | (Optional) A specific voice dial peer. The output displays detailed information about that dial peer. |
| busy-trigger-counter | (Optional) Displays the busy trigger call count on the VoIP dial peer. |
| summary | (Optional) Displays a short summary of each voice dial peer. |
| voip system | (Optional) Displays information about the VoIP dial peer. |

Command Default

If both the *number* argument and **summary** keyword are omitted, the output displays detailed information about all voice dial peers.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

| Release | Modification |
|-----------|---|
| 11.3(1)T | This command was introduced. |
| 11.3(1)MA | This command was modified. The summary keyword was added for the Cisco MC3810. |
| 12.0(3)XG | This command was implemented for Voice over Frame Relay (VoFR) on the Cisco 2600 series and Cisco 3600 series. |
| 12.0(4)T | This command was implemented for VoFR on the Cisco 7200 series. |
| 12.1(3)T | This command was implemented for modem pass-through over VoIP on the Cisco AS5300. |
| 12.2(2)XB | This command was modified to support VoiceXML applications. |
| 12.2(4)T | This command was implemented on the Cisco 1750. |
| 12.2(8)T | This command was implemented on the Cisco 1751, Cisco 2600 series, Cisco 3600 series, Cisco 3725, and Cisco 3745. |
| 12.2(2)XN | This command was modified. Support for enhanced Media Gateway Control Protocol (MGCP) voice gateway interoperability was added to Cisco CallManager 3.1 for the Cisco 2600 series, Cisco 3600 series, and Cisco VG200. |
| 12.2(11)T | This command was integrated into Cisco IOS Release 12.2(11)T and Cisco CallManager 3.2 and implemented on the Cisco IAD2420. The command was enhanced to display configuration information for bandwidth, video codec, and rtp payload-type for H.263+ and H.264 video codec. |

| Release | Modification |
|-----------|--|
| 12.4(22)T | This command was modified. This command was enhanced to display the current configuration state of the history-info header. Command output was updated to show IPv6 information. |
| 15.0(1)XA | This command was modified. The output was enhanced to show the logical partitioning class of restriction (LPCOR) policy for outgoing calls. |
| 15.1(1)T | This command was integrated into Cisco IOS Release 15.1(1)T. |
| 15.1(3)T | This command was modified. The output was enhanced to display information about the bind at the dial-peer level and to display the connection status of Foreign Exchange Office (FXO) ports. |

Usage Guidelines

Use this command to display the configuration for all VoIP and POTS dial peers configured for a gateway. To display configuration information for only one specific dial peer, use the *number* argument. To display summary information for all dial peers, use the **summary** keyword.

Examples

The following is sample output from the **show dial-peer voice** command for a POTS dial peer:

```
Router# show dial-peer voice 100

VoiceEncapPeer3201
peer type = voice, information type = video,
description = '',
tag = 3201, destination-pattern = `86001',
answer-address = '', preference=0,
CLID Restriction = None
CLID Network Number = ''
CLID Second Number sent
CLID Override RDNIS = disabled,
source carrier-id = '',target carrier-id = '',
source trunk-group-label = '',target trunk-group-label = '',
numbering Type = `unknown'
group = 3201, Admin state is up, Operation state is up,
Outbound state is up,
incoming called-number = '', connections/maximum = 0/unlimited,
DTMF Relay = disabled,
URI classes:
    Destination =
huntstop = disabled,
in bound application associated: 'DEFAULT'
out bound application associated: ''
dnis-map =
permission :both
    incoming COR list:maximum capability
outgoing COR list:minimum requirement
Translation profile (Incoming):
Translation profile (Outgoing):
incoming call blocking:
translation-profile = ''
disconnect-cause = `no-service'
advertise 0x40 capacity_update_timer 25 addrFamily 4 oldAddrFamily 4
type = pots, prefix = '',
forward-digits 4
session-target = '', voice-port = `2/0:23',
direct-inward-dial = enabled,
digit_strip = enabled,
```

show dial-peer voice

```

register E.164 number with H323 GK and/or SIP Registrar = TRUE
fax rate = system,   payload size = 20 bytes
supported-language = ''
preemption level = `routine'
bandwidth:
    maximum = 384 KBits/sec, minimum = 64 KBits/sec
voice class called-number:
    inbound = `', outbound = `1'
Time elapsed since last clearing of voice call statistics never
    Connect Time = 0, Charged Units = 0,
Successful Calls = 0, Failed Calls = 0, Incomplete Calls = 0
Accepted Calls = 0, Refused Calls = 0,
Last Disconnect Cause is "",
Last Disconnect Text is "",
Last Setup Time = 0.

```

The following is sample output from this command for a VoIP dial peer:

```
Router# show dial-peer voice 101
```

```

VoiceOverIpPeer101
peer type = voice, system default peer = FALSE, information type = voice,
description = `',
tag = 1234, destination-pattern = `',
voice reg type = 0, corresponding tag = 0,
allow watch = FALSE
answer-address = `', preference=0,
CLID Restriction = None
CLID Network Number = ` '
CLID Second Number sent
CLID Override RDNIS = disabled,
rtp-ssrc mux = system
source carrier-id = `', target carrier-id = `',
source trunk-group-label = `', target trunk-group-label = `',
numbering Type = `unknown'
group = 1234, Admin state is up, Operation state is down,
incoming called-number = `', connections/maximum = 0/unlimited,
DTMF Relay = disabled,
modem transport = system,
URI classes:
Incoming (Request) =
Incoming (Via) =
Incoming (To) =
Incoming (From) =
Destination =
huntstop = disabled,
in bound application associated: 'DEFAULT'
out bound application associated: ''
dnis-map =
permission :both
incoming COR list:maximum capability
outgoing COR list:minimum requirement
outgoing LPCOR:
Translation profile (Incoming):
Translation profile (Outgoing):
incoming call blocking:
translation-profile = ` '
disconnect-cause = `no-service'
advertise 0x40 capacity_update_timer 25 addrFamily 4 oldAddrFamily 4
mailbox selection policy: none
type = voip, session-target = `',
technology prefix:
settle-call = disabled
ip media DSCP = ef, ip media rsvp-pass DSCP = ef

```

```
ip media rsvp-fail DSCP = ef, ip signaling DSCP = af31,
ip video rsvp-none DSCP = af41, ip video rsvp-pass DSCP = af41
ip video rsvp-fail DSCP = af41,
ip defending Priority = 0, ip preemption priority = 0
ip policy locator voice:
ip policy locator video:
UDP checksum = disabled,
session-protocol = sipv2, session-transport = system,
req-qos = best-effort, acc-qos = best-effort,
req-qos video = best-effort, acc-qos video = best-effort,
req-qos audio def bandwidth = 64, req-qos audio max bandwidth = 0,
req-qos video def bandwidth = 384, req-qos video max bandwidth = 0,
RTP dynamic payload type values: NTE = 101
Cisco: NSE=100, fax=96, fax-ack=97, dtmf=121, fax-relay=122
CAS=123, TTY=119, ClearChan=125, PCM switch over u-law=0,
A-law=8, GSMAMR-NB=117 iLBC=116, AAC-ld=114, iSAC=124
lmr_tone=0, nte_tone=0
h263+=118, h264=119
G726r16 using static payload
G726r24 using static payload
RTP comfort noise payload type = 19
fax rate = voice, payload size = 20 bytes
fax protocol = system
fax-relay ecm enable
Fax Relay ans enabled
Fax Relay SG3-to-G3 Enabled (by system configuration)
fax NSF = 0xAD0051 (default)
codec = g729r8, payload size = 20 bytes,
video codec = None
voice class codec = ``
voice class sip session refresh system
voice class sip rsvp-fail-policy voice post-alert mandatory keep-alive interval 30
voice class sip rsvp-fail-policy voice post-alert optional keep-alive interval 30
voice class sip rsvp-fail-policy video post-alert mandatory keep-alive interval 30
voice class sip rsvp-fail-policy video post-alert optional keep-alive interval 30
text relay = disabled
Media Setting = forking (disabled) flow-through (global)
Expect factor = 10, Icpif = 20,
Playout Mode is set to adaptive,
Initial 60 ms, Max 1000 ms
Playout-delay Minimum mode is set to default, value 40 ms
Fax nominal 300 ms
Max Redirects = 1, signaling-type = cas,
VAD = enabled, Poor QOV Trap = disabled,
Source Interface = NONE
voice class sip url = system,
voice class sip tel-config url = system,
voice class sip rellxx = system,
voice class sip anat = system,
voice class sip outbound-proxy = "system",
voice class sip associate registered-number = system,
voice class sip asserted-id system,
voice class sip privacy system
voice class sip e911 = system,
voice class sip history-info = system,
voice class sip reset timer expires 183 = system,
voice class sip pass-thru headers = system,
voice class sip pass-thru content unsupp = system,
voice class sip pass-thru content sdp = system,
voice class sip copy-list = system,
voice class sip g729 annexb-all = system,
voice class sip early-offer forced = system,
voice class sip negotiate cisco = system,
voice class sip block 180 = system,
```

```

voice class sip block 183 = system,
voice class sip block 181 = system,
voice class sip preloaded-route = system,
voice class sip random-contact = system,
voice class sip random-request-uri validate = system,
voice class sip call-route p-called-party-id = system,
voice class sip call-route history-info = system,
voice class sip privacy-policy send-always = system,
voice class sip privacy-policy passthru = system,
voice class sip privacy-policy strip history-info = system,
voice class sip privacy-policy strip diversion = system,
voice class sip map resp-code 181 = system,
voice class sip bind control = enabled, 9.42.28.29,
voice class sip bind media = enabled, 9.42.28.29,
voice class sip bandwidth audio = system,
voice class sip bandwidth video = system,
voice class sip encap clear-channel = system,
voice class sip error-code-override options-keepalive failure = system,
voice class sip calltype-video = false
voice class sip registration passthrough = System
voice class sip authenticate redirecting-number = system,
redirect ip2ip = disabled
local peer = false
probe disabled,
Secure RTP: system (use the global setting)
voice class perm tag = ``
Time elapsed since last clearing of voice call statistics never
Connect Time = 0, Charged Units = 0,
Successful Calls = 0, Failed Calls = 0, Incomplete Calls = 0
Accepted Calls = 0, Refused Calls = 0,
Last Disconnect Cause is "",
Last Disconnect Text is "",
Last Setup Time = 0.
Last Disconnect Time = 0.

```

When there is no Dial-peer level bind -

```

voice class sip bind control = system,
voice class sip bind media = system,

```

The following is sample output from the **show dial-peer voice summary** command that shows connected FXO port 0/2/0 (the last entry) has OUT STAT set to “up,” which indicates that the POTS dial peer can be used for an outgoing call. If this port is disconnected, the status changes in the output so that the OUT STAT field reports “down,” and the POTS dial peer cannot be used for an outgoing call.

**Note**

Beginning in Cisco IOS Release 15.1(3)T, there is improved status monitoring of FXO ports—any time an FXO port is connected or disconnected, a message is displayed to indicate the status change. For example, the following message is displayed to report that a cable has been connected, and the status is changed to “up” for FXO port 0/2/0:

```

000118: Jul 14 18:06:05.122 EST: %LINK-3-UPDOWN: Interface Foreign Exchange Office 0/2/0,
changed state to operational status up due to cable reconnection

```

```

Router# show dial-peer voice summary

```

```

dial-peer hunt 0
          AD
TAG      TYPE  MIN  OPER PREFIX  DEST-PATTERN  PRE PASS  OUT
KEEPALIVE  FER THRU SESS-TARGET  STAT PORT
39275- voip up   up      .T          0  syst ipv4:172.18.108.26
82

```

```

8880 pots up up 8880 0 up 2/0/0
8881 pots up up 8881 0 up 2/0/1
8882 pots up up 8882 0 up 2/0/2
8883 pots up up 8883 0 up 2/0/3
8884 pots up up 8884 0 up 2/0/4
8885 pots up up 8885 0 up 2/0/5
8886 pots up up 8886 0 up 2/0/6
8887 pots up up 8887 0 up 2/0/7
8888- pots up up 0 down 0/3/0:23
888
65033- pots up up 650332 0 up 0/2/0
52

```

Table 70 describes the significant fields shown in the displays, in alphabetical order.

Table 70 *show dial-peer voice Field Descriptions*

| Field | Description |
|---------------------------|--|
| Accepted Calls | Number of calls accepted from this peer since system startup. |
| acc-qos | Lowest acceptable quality of service configured for calls for this peer. |
| Admin state | Administrative state of this peer. |
| answer-address | Answer address configured for this dial peer. |
| bandwidth maximum/minimum | The maximum and minimum bandwidth, in Kb/s. |
| Charged Units | Total number of charging units that have applied to this peer since system startup, in hundredths of a second. |
| CLID Restriction | Indicates if Calling Line ID (CLID) restriction is enabled. |
| CLID Network Number | Displays the network number sent as CLID, if configured. |
| CLID Second Number sent | Displays whether a second calling number is stripped from the call setup. |
| CLID Override RDNIS | Indicates whether the CLID is overridden by the redirecting number. |
| codec | Default voice codec rate of speech. |
| Connect Time | Accumulated connect time to the peer since system startup for both incoming and outgoing calls, in hundredths of a second. |
| connections/maximum | Indicates the maximum number of call connections per peer. |
| Destination | Indicates the voice class that is used to match the destination URL. |
| destination-pattern | Destination pattern (telephone number) for this peer. |
| digit_strip | Indicates if digit stripping is enabled. |
| direct-inward-dial | Indicates if direct inward dial is enabled. |
| disconnect-cause | Indicates the disconnect cause code to be used when an incoming call is blocked. |
| dnis-map | Name of the dialed-number identification service (DNIS) map. |
| DTMF Relay | Indicates if dual-tone multifrequency (DTMF) relay is enabled. |
| Expect factor | User-requested expectation factor of voice quality for calls through this peer. |
| Failed Calls | Number of failed call attempts to this peer since system startup. |

Table 70 *show dial-peer voice Field Descriptions (continued)*

| Field | Description |
|----------------------------------|---|
| fax rate | Fax transmission rate configured for this peer. |
| forward-digits | Indicates the destination digits to be forwarded of this peer. |
| group | Group number associated with this peer. |
| huntstop | Indicates whether dial-peer hunting is turned on, by the huntstop command, for this dial peer. |
| Icpif | Configured Impairment/Calculated Planning Impairment Factor (ICPIF) value for calls sent by a dial peer. |
| in bound application associated | Interactive voice response (IVR) application that is configured to handle inbound calls to this dial peer. |
| incall-number | Full E.164 telephone number to be used to identify the dial peer. |
| incoming call blocking | Indicates the incoming call blocking setup of this peer. |
| incoming called-number | Indicates the incoming called number if it has been set. |
| incoming COR list | Indicates the level of Class of Restrictions for incoming calls of this peer. |
| Incomplete Calls | Indicates the number of outgoing disconnected calls with the user busy (17), no user response (18), or no answer (19) cause code. |
| information type | Information type for this call (voice, fax, video). |
| Last Disconnect Cause | Encoded network cause associated with the last call. This value is updated whenever a call is started or cleared and depends on the interface type and session protocol being used on this interface. |
| Last Disconnect Text | ASCII text describing the reason for the last call termination. |
| Last Setup Time | Value of the system uptime when the last call to this peer was started. |
| Modem passthrough | Modem pass-through signaling method is named signaling event (NSE). |
| numbering Type | Indicates the numbering type for a peer call leg. |
| Operation state | Operational state of this peer. |
| outgoing COR list | Indicates the level of Class of Restrictions for outgoing calls of this peer. |
| outgoing LPCOR | Setting of the lpcor outgoing command. |
| out bound application associated | The voice application that is configured to handle outbound calls from this dial peer. Outbound calls are handed off to the named application. |
| Outbound state | Indicates the current outbound status of a POTS peer. |
| payload size | Indicates the size (in bytes) of the payload of the fax rate or codec setup. |
| payload type | NSE payload type. |
| peer type | Dial peer type (voice, data). |
| permission | Configured permission level for this peer. |
| Poor QOV Trap | Indicates if poor quality of voice trap messages is enabled. |

Table 70 *show dial-peer voice Field Descriptions (continued)*

| Field | Description |
|---|--|
| preemption level | Indicates the call preemption level of this peer. |
| prefix | Indicates dialed digits prefix of this peer. |
| Redundancy | Packet redundancy (RFC 2198) for modem traffic. |
| Refused Calls | Number of calls from this peer refused since system startup. |
| register E.164 number with H.323 GK and/or SIP Registrar | Indicates the "register e.164" option of this peer. |
| req-qos | Configured requested quality of service for calls for this dial peer. |
| session-target | Session target of this peer. |
| session-protocol | Session protocol to be used for Internet calls between local and remote routers through the IP backbone. |
| source carrier-id | Indicates the source carrier ID of this peer that will be used to match the source carrier ID of an incoming call. |
| source trunk-group label | Indicates the source trunk group label of this peer that can be used to match the source trunk group label of an incoming call. |
| Successful Calls | Number of completed calls to this peer. |
| supported-language | Indicates the list of supported languages of this peer. |
| tag | Unique dial peer ID number. |
| target carrier-id | Indicates the target carrier ID of this peer that will be used to match the target carrier ID for an outgoing call. |
| target-trunkgroup-label | Indicates the target trunk group label of this peer that can be used to match the target trunk group label of an outgoing call. |
| Time elapsed since last clearing of voice call statistics | Elapsed time between the current time and the time when the clear dial-peer voice command was executed. |
| Translation profile (Incoming) | Indicates the translation profile for incoming calls. |
| Translation profile (Outgoing) | Indicates the translation profile for outgoing calls. |
| translation-profile | Indicates the number translation profile of this peer. |
| type | Indicates the peer encapsulation type (pots, voip, vofr, voatm or mmoip). |
| VAD | Whether voice activation detection (VAD) is enabled for this dial peer. |
| voice class called-number inbound/outbound | Indicates the voice-class called number inbound or outbound setup of this peer. |
| voice class sip history-info | Indicates the configuration state of the history-info header. If the history-info header is not configured for the dial peer, this field is set to system. If the history-info header is enabled on this dial peer, this field is set to enable. If the history-info header is disabled on this dial peer, this field is set to disable. |

Table 70 *show dial-peer voice Field Descriptions (continued)*

| Field | Description |
|----------------------|--|
| voice class sip bind | Indicates the configuration state of the bind address. If the bind is configured for the global, this field is sent to system. If the bind address is enabled on this dial peer, this field is set to enabled. |
| voice-port | Indicates the voice interface setting of this POTS peer. |

The following is sample output from this command with the **summary** keyword:

```
Router# show dial-peer voice summary

dial-peer hunt 0

          PASS
TAG TYPE  ADMIN OPER PREFIX  DEST-PATTERN  PREF THRU SESS-TARGET  PORT
100 pots  up    up           5550112       0   syst ipv4:10.10.1.1
101 voip  up    up           5550134       0   syst ipv4:10.10.1.1
99  voip  up    down        0             0   syst
33  pots  up    down        0             0
```

[Table 71](#) describes the significant fields shown in the display.

Table 71 *show dial-peer voice summary Field Descriptions*

| Field | Description |
|----------------|--|
| dial-peer hunt | Hunt group selection order that is defined for the dial peer by the dial-peer hunt command. |
| TAG | Unique identifier assigned to the dial peer when it was created. |
| TYPE | Type of dial peer (mmoip, pots, voatm, voifr, or voip). |
| ADMIN | Whether the administrative state is up or down. |
| OPER | Whether the operational state is up or down. |
| PREFIX | Prefix that is configured in the dial peer by the prefix command. |
| DEST-PATTERN | Destination pattern that is configured in the dial peer by the destination-pattern command. |
| PREF | Hunt group preference that is configured in the dial peer by the preference command. |
| PASS THRU | Modem pass-through method that is configured in the dial peer by the modem passthrough command. |
| SESS-TARGET | Destination that is configured in the dial peer by the session target command. |
| PORT | Router voice port that is configured for the dial peer. Valid only for POTS dial peers. |

Related Commands

| Command | Description |
|--------------------------------|---------------------------------------|
| show call active voice | Displays the VoIP active call table. |
| show call history voice | Displays the VoIP call history table. |

| Command | Description |
|------------------------------------|---|
| show dialplan incall number | Displays which POTS dial peer is matched for a specific calling number or voice port. |
| show dialplan number | Displays which dial peer is reached when a specific telephone number is dialed. |
| show num-exp | Displays how the number expansions are configured in VoIP. |
| show voice port | Displays configuration information about a specific voice port. |

show dmvpn

To display Dynamic Multipoint VPN (DMVPN)-specific session information, use the **show dmvpn** command in privileged EXEC mode.

```
show dmvpn [ipv4 [vrf vrf-name] | ipv6 [vrf vrf-name]] [debug-condition | [interface tunnel
number | peer {nbma ip-address | network network-mask | tunnel ip-address}] [static]
[detail]]
```

| Syntax | Description |
|------------------------------------|--|
| ipv4 | (Optional) Displays information about IPv4 private networks. |
| vrf <i>vrf-name</i> | (Optional) Displays information based on the specified virtual routing and forwarding (VRF) instance. |
| ipv6 | (Optional) Displays information about IPv6 private networks. |
| debug-condition | (Optional) Displays DMVPN conditional debugging. |
| interface | (Optional) Displays DMVPN information based on a specific interface. |
| tunnel | (Optional) Displays DMVPN information based on the peer Virtual Private Network (VPN) address. |
| <i>number</i> | (Optional) The tunnel address for a DMVPN peer. |
| peer | (Optional) Displays information for a specific DMVPN peer. |
| nbma | Displays DMVPN information based on nonbroadcast multiaccess (NBMA) addresses. |
| <i>ip-address</i> | The DMVPN peer IP address. |
| network <i>network-mask</i> | Displays DMVPN information based on a specific destination network and mask address. |
| static | (Optional) Displays only static DMVPN information. |
| detail | (Optional) Displays detail DMVPN information for each session, including Next Hop Server (NHS) and NHS status, crypto session information, and socket details. |

Command Default Information is displayed for all DMVPN-specific sessions.

Command Modes Privileged EXEC (#)

| Command History | Release | Modification |
|-----------------|-----------|---|
| | 12.4(9)T | This command was introduced. |
| | 12.4(20)T | This command was modified. The following were added: ipv4 , ipv6 , <i>ipv6-address</i> , network , and <i>ipv6-address</i> . |
| | 12.4(22)T | This command was modified. The output of this command was extended to display the NHRP group received from the spoke and the Quality of Service (QoS) policy applied to the spoke tunnel. |

Usage Guidelines

Use this command to obtain DMVPN-specific session information. By default, summary information will be displayed.

When the **detail** keyword is used, command output will include information from the **show crypto session detail** command, including inbound and outbound security parameter indexes (SPIs) and the **show crypto socket** command.

Examples

The following example shows sample summary output:

```
Router# show dmvpn

Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
         N - NATed, L - Local, X - No Socket
         # Ent --> Number of NHRP entries with same NBMA peer

! The line below indicates that the sessions are being displayed for Tunnel1.
! Tunnel1 is acting as a spoke and is a peer with three other NBMA peers.

Tunnel1, Type: Spoke, NBMA Peers: 3,

# Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
-----
      2    192.0.2.21    192.0.2.116  IKE    3w0d D
      1    192.0.2.102    192.0.2.11  NHRP  02:40:51 S
      1    192.0.2.225    192.0.2.10   UP     3w0d S

Tunnel2, Type: Spoke, NBMA Peers: 1,
# Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
-----
      1    192.0.2.25    192.0.2.171  IKE    never S
```

[Table 72](#) describes the significant fields shown in the display.

Table 72 show dmvpn Field Descriptions

| Field | Description |
|-----------------|--|
| # Ent | The number of Next Hop Routing Protocol (NHRP) entries in the current session. |
| Peer NBMA Addr | The remote NBMA address. |
| Peer Tunnel Add | The remote tunnel endpoint IP address. |
| State | The state of the DMVPN session. The DMVPN session is either up or down. If the DMVPN state is down, the reason for the down state error is displayed—Internet Key Exchange (IKE), IPsec, or NHRP. |
| UpDn Tm | Displays how long the session has been in the current state. |
| Attrib | Displays any associated attributes of the current session. One of the following attributes will be displayed—dynamic (D), static (S), incomplete (I), Network Address Translation (NAT) for the peer address, or NATed, (N), local (L), no socket (X). |

The following example shows output of the **show dmvpn** command with the **detail** keyword:

```
Router# show dmvpn detail

Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        # Ent --> Number of NHRP entries with same NBMA peer
----- Interface Tunnel1 info: -----
Intf. is up, Line Protocol is up, Addr. is 192.0.2.5
  Source addr: 192.0.2.229, Dest addr: MGRE
  Protocol/Transport: "multi-GRE/IP", Protect "gre_prof",
Tunnel VRF "" ip vrf forwarding ""
NHRP Details: NHS: 192.0.2.10 RE 192.0.2.11 E
Type: Spoke, NBMA Peers: 4
# Ent Peer NBMA Addr Peer Tunnel Add State UpDn Tm Attrb Target Network
-----
      2      192.0.2.21      192.0.2.116      UP 00:14:59 D      192.0.2.118/24
                                         UP 00:14:59 D      192.0.2.116/32

IKE SA: local 192.0.2.229/500 remote 192.0.2.21/500 Active
      Capabilities:(none) connid:1031 lifetime:23:45:00
Crypto Session Status: UP-ACTIVE
fvrf: (none)
IPSEC FLOW: permit 47 host 192.0.2.229 host 192.0.2.21
      Active SAs: 2, origin: crypto map
      Inbound: #pkts dec'ed 1 drop 0 life (KB/Sec) 4494994/2700
      Outbound: #pkts enc'ed 1 drop 0 life (KB/Sec) 4494994/2700
      Outbound SPI : 0xD1EA3C9B, transform : esp-3des esp-sha-hmac
      Socket State: Open

# Ent Peer NBMA Addr Peer Tunnel Add State UpDn Tm Attrb Target Network
-----
      1      192.0.2.229      192.0.2.5      UP 00:15:00 DLX      192.0.2.5/32

# Ent Peer NBMA Addr Peer Tunnel Add State UpDn Tm Attrb Target Network
-----
      1      192.0.2.102      192.0.2.11 NHRP 02:55:47 S      192.0.2.11/32

IKE SA: local 192.0.2.229/4500 remote 192.0.2.102/4500 Active
      Capabilities:N connid:1028 lifetime:11:45:37
Crypto Session Status: UP-ACTIVE
fvrf: (none)
IPSEC FLOW: permit 47 host 192.0.2.229 host 192.0.2.102
      Active SAs: 2, origin: crypto map
      Inbound: #pkts dec'ed 199056 drop 393401 life (KB/Sec) 4560270/1524
      Outbound: #pkts enc'ed 416631 drop 10531 life (KB/Sec) 4560322/1524
      Outbound SPI : 0x9451AF5C, transform : esp-3des esp-sha-hmac
      Socket State: Open

# Ent Peer NBMA Addr Peer Tunnel Add State UpDn Tm Attrb Target Network
-----
      1      192.0.2.225      192.0.2.10      UP      3w0d S      192.0.2.10/32

IKE SA: local 192.0.2.229/500 remote 192.0.2.225/500 Active
      Capabilities:(none) connid:1030 lifetime:03:46:44
Crypto Session Status: UP-ACTIVE
fvrf: (none)
IPSEC FLOW: permit 47 host 192.0.2.229 host 192.0.2.225
      Active SAs: 2, origin: crypto map
      Inbound: #pkts dec'ed 430261 drop 0 life (KB/Sec) 4415197/3466
      Outbound: #pkts enc'ed 406232 drop 4 life (KB/Sec) 4415197/3466
      Outbound SPI : 0xAF3E15F2, transform : esp-3des esp-sha-hmac
      Socket State: Open

----- Interface Tunnel2 info: -----
```

```

Intf. is up, Line Protocol is up, Addr. is 192.0.2.172
  Source addr: 192.0.2.20, Dest addr: MGRE
  Protocol/Transport: "multi-GRE/IP", Protect "gre_prof",
Tunnel VRF "" ip vrf forwarding ""

NHRP Details: NHS:          192.0.2.171  E

Type: Spoke, NBMA Peers: 1
# Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb   Target Network
-----
  1    192.0.2.25    192.0.2.171  IKE    never  S          192.0.2.171/32

IKE SA: local 192.0.2.20/500 remote 192.0.2.25/500 Inactive
      Capabilities:(none) connid:0 lifetime:0
IKE SA: local 192.0.2.20/500 remote 192.0.2.25/500 Inactive
      Capabilities:(none) connid:0 lifetime:0
Crypto Session Status: DOWN-NEGOTIATING
fvrf: (none)
IPSEC FLOW: permit 47 host 192.0.2.20 host 192.0.2.25
      Active SAs: 0, origin: crypto map
      Inbound:  #pkts dec'ed 0 drop 0 life (KB/Sec) 0/0
      Outbound: #pkts enc'ed 0 drop 436431 life (KB/Sec) 0/0
      Outbound SPI : 0x      0, transform :
      Socket State: Closed

Pending DMVPN Sessions:
!There are no pending DMVPN sessions.

```

The following example shows output of the **show dmvpn** command with the **detail** keyword. This example displays the NHRP group received from the spoke and the QoS policy applied to the spoke tunnel:

```

Router# show dmvpn detail
Legend: Attrb --> S - Static, D - Dynamic, I - Incompletea
      N - NATed, L - Local, X - No Socket
      # Ent --> Number of NHRP entries with same NBMA peer

----- Interface Tunnel0 info: -----
Intf. is up, Line Protocol is up, Addr. is 10.0.0.1
  Source addr: 172.17.0.1, Dest addr: MGRE
  Protocol/Transport: "multi-GRE/IP", Protect "dmvpn-profile",
Tunnel VRF "", ip vrf forwarding ""

NHRP Details:
Type:Hub, NBMA Peers:2
# Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb   Target Network
-----
  1    172.17.0.2    10.0.0.2    UP 00:19:57 D          10.0.0.2/32
NHRP group: test-group-0
Output QoS service-policy applied: queueing

IKE SA: local 172.17.0.1/500 remote 172.17.0.2/500 Active
Crypto Session Status: UP-ACTIVE
fvrf: (none), Phase1_id: 172.17.0.2
IPSEC FLOW: permit 47 host 172.17.0.1 host 172.17.0.2
      Active SAs: 2, origin: crypto map
      Outbound SPI : 0x44E4E634, transform : esp-des esp-sha-hmac
      Socket State: Open
IKE SA: local 172.17.0.1/500 remote 172.17.0.2/500 Active
IPSEC FLOW: permit 47 host 172.17.0.1 host 172.17.0.2
      Active SAs: 2, origin: crypto map
      Outbound SPI : 0x44E4E634, transform : esp-des esp-sha-hmac
      Socket State: Open
# Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb   Target Network

```

```

-----
      1      172.17.0.3      10.0.0.3      UP 00:02:21 D      10.0.0.3/32
NHRP group: test-group-0
Output QoS service-policy applied: queueing

IKE SA: local 172.17.0.1/500 remote 172.17.0.3/500 Active
Crypto Session Status: UP-ACTIVE
fvrf: (none), Phase1_id: 172.17.0.3
IPSEC FLOW: permit 47 host 172.17.0.1 host 172.17.0.3
      Active SAs: 2, origin: crypto map
      Outbound SPI : 0xBF13C9CC, transform : esp-des esp-sha-hmac
      Socket State: Open
IKE SA: local 172.17.0.1/500 remote 172.17.0.3/500 Active
IPSEC FLOW: permit 47 host 172.17.0.1 host 172.17.0.3
      Active SAs: 2, origin: crypto map
      Outbound SPI : 0xBF13C9CC, transform : esp-des esp-sha-hmac
      Socket State: Open

----- Interface Tunnel1 info: -----
Intf. is up, Line Protocol is up, Addr. is 11.0.0.1
      Source addr: 172.17.0.1, Dest addr: MGRE
      Protocol/Transport: "multi-GRE/IP", Protect "dmvpn-profile",
Tunnel VRF "", ip vrf forwarding ""

NHRP Details:
Type:Hub, NBMA Peers:1
# Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb      Target Network
-----
      1      172.17.0.2      11.0.0.2      UP 00:20:01 D      11.0.0.2/32
NHRP group: test-group-1
Output QoS service-policy applied: queueing

```

Pending DMVPN Sessions:

The following example shows DMVPN debug-condition information:

Router# **show dmvpn debug-condition**

```

NBMA addresses under debug are:
Interfaces under debug are:
Tunnel101,
Crypto DMVPN filters:
Interface = Tunnel101
DMVPN Conditional debug context unmatched flag: OFF

```

Related Commands

| Command | Description |
|-----------------------------------|--|
| debug dmvpn | Debugs DMVPN sessions. |
| show crypto session detail | Displays detailed status information for active crypto sessions. |
| show crypto socket | Lists crypto sockets. |
| show policy-map mgre | Displays statistics about a specific QoS policy as it is applied to a tunnel endpoint. |

show eigrp address-family accounting

To display prefix accounting information for Enhanced Interior Gateway Routing Protocol (EIGRP) processes, use the **show eigrp address-family accounting** command in user EXEC or privileged EXEC mode.

```
show eigrp address-family {ipv4 | ipv6} [vrf vrf-name] [autonomous-system-number] [multicast]
accounting
```

| Syntax Description | | |
|---------------------------------|--|--|
| ipv4 | Selects the IPv4 protocol address family. | |
| ipv6 | Selects the IPv6 protocol address family. | |
| vrf <i>vrf-name</i> | (Optional) Displays information about the specified VRF. This keyword/argument pair is available only for IPv4 configurations. | |
| <i>autonomous-system-number</i> | (Optional) Autonomous system number. | |
| multicast | (Optional) Displays information about multicast instances. | |

| Command Modes | |
|---------------------|--|
| User EXEC (>) | |
| Privileged EXEC (#) | |

| Command Default | |
|---|--|
| Prefix accounting information for all EIGRP processes is displayed. | |

| Command History | Release | Modification |
|-----------------|--------------------------|---|
| | 15.0(1)M | This command was introduced. |
| | 12.2(33)SRE | This command was integrated into Cisco IOS Release 12.2(33)SRE. |
| | 12.2(33)XNE | This command was integrated into Cisco IOS Release 12.2(33)XNE. |
| | Cisco IOS XE Release 2.5 | This command was integrated into Cisco IOS XE Release 2.5. |

Usage Guidelines This command can be used to display information about EIGRP named configurations and EIGRP autonomous-system (AS) configurations.

This command displays the same information as the **show ip eigrp accounting** command. Cisco recommends using the **show eigrp address-family accounting** command.

Examples The following example shows how to display EIGRP prefix accounting information for autonomous-system 22:

```
Router# show eigrp address-family ipv4 22 accounting

EIGRP-IPv4 VR(saf) Accounting for AS(22)/ID(10.0.0.1)
Total Prefix Count: 3 States: A-Adjacency, P-Pending, D-Down
State Address/Source Interface Prefix Restart Restart/
```


show eigrp address-family accounting

| | | | Count | Count | Reset(s) |
|---|----------|-------|-------|-------|----------|
| A | 10.0.0.2 | Et0/0 | 2 | 0 | 0 |
| P | 10.0.2.4 | Se2/0 | 0 | 2 | 114 |
| D | 10.0.1.3 | Et0/0 | 0 | 3 | 0 |

Table 73 describes the significant fields shown in the display.

Table 73 *show eigrp address-family accounting Field Descriptions*

| Field | Description |
|-------------------------------|---|
| IP-EIGRP accounting for AS... | Identifies the EIGRP instance, AS number, router ID, and table ID. |
| Total Prefix Count | Number of distinct prefixes that are present in this autonomous system. |
| State | State of the given neighbor: Adjacency, Pending, or Down. |
| Address/Source | IP address of the neighbor. |
| Interface | Interface on which the neighbor is connected. |
| Prefix Count | Number of prefixes that are advertised by this neighbor. |
| Restart Count | Number of times this neighbor has been restarted due to exceeding prefix limits. |
| Restart/Reset(s) | Time remaining until the neighbor will be restarted (if in Pending state) or until the restart count will be cleared (if in Adjacency state.) |

Related Commands

| Command | Description |
|---|---|
| show eigrp address-family events | Displays information about EIGRP events. |
| show eigrp address-family interfaces | Displays information about interfaces configured for EIGRP. |
| show eigrp address-family neighbors | Displays the neighbors discovered by EIGRP. |
| show eigrp address-family sia-event | Displays information about EIGRP SIA events. |
| show eigrp address-family sia-statistics | Displays information about EIGRP SIA statistics. |
| show eigrp address-family timers | Displays information about EIGRP timers and expiration times. |
| show eigrp address-family topology | Displays entries in the EIGRP topology table. |
| show eigrp address-family traffic | Displays the number of EIGRP packets sent and received. |

show eigrp address-family events

To display information about Enhanced Interior Gateway Routing Protocol (EIGRP) address-family events, use the **show eigrp address-family events** command in user EXEC or privileged EXEC mode.

```
show eigrp address-family {ipv4 | ipv6} [vrf vrf-name] [autonomous-system-number] [multicast]
events [starting-event-number ending-event-number] [errmsg [starting-event-number
ending-event-number]] [sia [starting-event-number ending-event-number]] [type]
```

Syntax Description

| | |
|---------------------------------|--|
| ipv4 | Selects the IPv4 protocol address family. |
| ipv6 | Selects the IPv6 protocol address family. |
| vrf <i>vrf-name</i> | (Optional) Displays information about the specified VRF. |
| <i>autonomous-system-number</i> | (Optional) Autonomous system number. |
| multicast | (Optional) Displays information about multicast instances. |
| <i>starting-event-number</i> | (Optional) Number of first event to display. |
| <i>ending-event-number</i> | (Optional) Number of last event to display. |
| errmsg | (Optional) Displays error message events. |
| sia | (Optional) Displays Stuck in Active (SIA) events. |
| type | (Optional) Displays the types of events being logged. |

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command Default

All EIGRP address-family events are displayed.

Command History

| Release | Modification |
|--------------------------|---|
| 15.0(1)M | This command was introduced. |
| 12.2(33)SRE | This command was integrated into Cisco IOS Release 12.2(33)SRE. |
| 12.2(33)XNE | This command was integrated into Cisco IOS Release 12.2(33)XNE. |
| Cisco IOS XE Release 2.5 | This command was integrated into Cisco IOS XE Release 2.5. |

Usage Guidelines

The event log is used by Cisco technical support to display a history of EIGRP internal events that are specific to a particular address family.

To display information about EIGRP service-family events, use the **show eigrp service-family events** command.

This command can be used to display information about EIGRP named configurations and EIGRP autonomous-system (AS) configurations.

This command displays the same information as the **show ip eigrp events** command. Cisco recommends using the **show eigrp address-family events** command.

Examples

The following example shows how to display EIGRP address-family events for autonomous-system 3:

```
Router# show eigrp address-family ipv4 3 events

Event information for AS 3:
1 15:37:47.015 Change queue emptied, entries: 1
2 15:37:47.015 Metric set: 10.0.0.0/24 307200
3 15:37:47.015 Update reason, delay: new if 4294967295
4 15:37:47.015 Update sent, RD: 10.0.0.0/24 4294967295
5 15:37:47.015 Update reason, delay: metric chg 4294967295
6 15:37:47.015 Update sent, RD: 10.0.0.0/24 4294967295
7 15:37:47.015 Route installed: 10.0.0.0/24 1.1.1.2
8 15:37:47.015 Route installing: 10.0.0.0/24 10.0.1.2
```

Related Commands

| Command | Description |
|---|---|
| show eigrp address-family accounting | Displays prefix accounting information for EIGRP processes. |
| show eigrp address-family interfaces | Displays information about interfaces configured for EIGRP. |
| show eigrp address-family neighbors | Displays the neighbors discovered by EIGRP. |
| show eigrp address-family sia-event | Displays information about EIGRP SIA events. |
| show eigrp address-family sia-statistics | Displays information about EIGRP SIA statistics. |
| show eigrp address-family timers | Displays information about EIGRP timers and expiration times. |
| show eigrp address-family topology | Displays entries in the EIGRP topology table. |
| show eigrp address-family traffic | Displays the number of EIGRP packets sent and received. |
| show eigrp service-family events | Displays information about EIGRP service-family events. |

show eigrp address-family interfaces

To display information about interfaces that are configured for Enhanced Interior Gateway Routing Protocol (EIGRP), use the **show eigrp address-family interfaces** command in user EXEC or privileged EXEC mode.

```
show eigrp address-family {ipv4 | ipv6} [vrf vrf-name] [autonomous-system-number] [multicast]
interfaces [detail] [interface-type interface-number]
```

| Syntax Description | | |
|--|--|--|
| ipv4 | Selects the IPv4 protocol address family. | |
| ipv6 | Selects the IPv6 protocol address family. | |
| vrf <i>vrf-name</i> | (Optional) Displays information about the specified VRF. | |
| <i>autonomous-system-number</i> | (Optional) Autonomous system number. | |
| multicast | (Optional) Displays information about multicast instances. | |
| detail | (Optional) Displays detailed information about EIGRP interfaces. | |
| <i>interface-type interface-number</i> | (Optional) Interface type and number to display. If unspecified, all enabled interfaces are displayed. | |

Command Default All enabled EIGRP interfaces are displayed.

Command Modes User EXEC (>)
Privileged EXEC (#)

| Command History | Release | Modification |
|-----------------|--------------------------|---|
| | 15.0(1)M | This command was introduced. |
| | 12.2(33)SRE | This command was integrated into Cisco IOS Release 12.2(33)SRE. |
| | 12.2(33)XNE | This command was integrated into Cisco IOS Release 12.2(33)XNE. |
| | Cisco IOS XE Release 2.5 | This command was integrated into Cisco IOS XE Release 2.5. |

Usage Guidelines Use the **show eigrp address-family interfaces** command to determine on which interfaces EIGRP is active and to learn EIGRP information about those interfaces.

If an interface is specified, only information about that interface is displayed. Otherwise, information about all interfaces on which EIGRP is running is displayed.

If an autonomous system is specified, only the routing process for the specified autonomous system is displayed. Otherwise, all EIGRP processes are displayed.

This command can be used to display information about EIGRP named configurations and EIGRP autonomous-system (AS) configurations.

This command displays the same information as the **show ip eigrp interfaces** command. Cisco recommends using the **show eigrp address-family interfaces** command.

Examples

The following example shows how to display information about EIGRP interfaces for autonomous-system 4453:

```
Router# show eigrp address-family ipv4 4453 interfaces

EIGRP-IPv4 VR(Virtual-name) Address-family Neighbors for AS(4453)
      Xmit Queue   Mean   Pacing Time   Multicast   Pending
Interface  Peers Un/Reliable SRTT   Un/Reliable   Flow Timer   Services
Se0        1      0/0       28     0/15         127         0
Se1        1      0/0       44     0/15         211         0
```

The following example shows how to display detailed information about Loopback interface 1 in autonomous-system 2:

```
Router# show eigrp address-family ipv4 2 interfaces detail Loopback1

EIGRP-IPv4 VR(saf2) Address-family Neighbors for AS(2)
      Xmit Queue   Mean   Pacing Time   Multicast   Pending
Interface  Peers Un/Reliable SRTT   Un/Reliable   Flow Timer   Services
Lo1        166    0/0       48     0/1         258         0
  Hello-interval is 5, Hold-time is 15
  Split-horizon is enabled
  Next xmit serial <none>
  Un/reliable mcasts: 0/0 Un/reliable ucasts: 10148/67233
  Mcast exceptions: 0 CR packets: 0 ACKs suppressed: 8719
  Retransmissions sent: 2696 Out-of-sequence rcvd: 594
  Interface has all stub peers
  Topology-ids on interface - 0
  Authentication mode is not set
```

Table 74 describes the significant fields shown in the display.

Table 74 show eigrp address-family interfaces Field Descriptions

| Field | Description |
|-------------------------|---|
| Interface | Interface over which EIGRP is configured. |
| Peers | Number of EIGRP neighbors connected on this interface. |
| Xmit Queue Un/Reliable | Number of packets remaining in the Unreliable and Reliable transmit queues. |
| Mean SRTT | Mean smooth round-trip time interval, in milliseconds. |
| Pacing Time Un/Reliable | Pacing time used to determine when reliable and unreliable EIGRP packets should be sent out of the interface. |
| Multicast Flow Timer | Maximum number of seconds the router sends multicast EIGRP packets. |
| Pending Services | Number of services in the packets in the transmit queue waiting to be sent. |
| CR packets | Packets marked for conditional Receive. |

Related Commands

| Command | Description |
|---|---|
| show eigrp address-family accounting | Displays prefix accounting information for EIGRP processes. |
| show eigrp address-family events | Displays information about EIGRP events. |
| show eigrp address-family neighbors | Displays the neighbors discovered by EIGRP. |
| show eigrp address-family sia-event | Displays information about EIGRP SIA events. |
| show eigrp address-family sia-statistics | Displays information about EIGRP SIA statistics. |
| show eigrp address-family timers | Displays information about EIGRP timers and expiration times. |
| show eigrp address-family topology | Displays entries in the EIGRP topology table. |
| show eigrp address-family traffic | Displays the number of EIGRP packets sent and received. |

show eigrp address-family neighbors

To display the neighbors that are discovered by Enhanced Interior Gateway Routing Protocol (EIGRP), use the **show eigrp address-family neighbors** command in user EXEC or privileged EXEC mode.

```
show eigrp address-family {ipv4 | ipv6} [vrf vrf-name] [autonomous-system-number] [multicast]
neighbors [static] [detail] [interface-type interface-number]
```

Syntax Description

| | |
|--|--|
| ipv4 | Selects the IPv4 protocol address family. |
| ipv6 | Selects the IPv6 protocol address family. |
| vrf <i>vrf-name</i> | (Optional) Displays information about the specified VRF. |
| <i>autonomous-system-number</i> | (Optional) Autonomous system number. |
| multicast | (Optional) Displays information about multicast instances. |
| static | (Optional) Displays static neighbors. |
| detail | (Optional) Displays detailed EIGRP neighbor information. |
| <i>interface-type interface-number</i> | (Optional) Interface type and number to display. If unspecified, all enabled interfaces are displayed. |

Command Default

Information about all neighbors discovered by EIGRP is displayed.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

| Release | Modification |
|--------------------------|---|
| 15.0(1)M | This command was introduced. |
| 12.2(33)SRE | This command was integrated into Cisco IOS Release 12.2(33)SRE. |
| 12.2(33)XNE | This command was integrated into Cisco IOS Release 12.2(33)XNE. |
| Cisco IOS XE Release 2.5 | This command was integrated into Cisco IOS XE Release 2.5. |

Usage Guidelines

Use the **show eigrp address-family neighbors** command to determine when neighbors become active and inactive. It is also useful for debugging certain types of transport problems.

This command can be used to display information about EIGRP named configurations and EIGRP autonomous-system (AS) configurations.

This command displays the same information as the **show ip eigrp neighbors** command. Cisco recommends using the **show eigrp address-family neighbors** command.

Examples

The following example shows how to display neighbors that are discovered by EIGRP:

```
Router# show eigrp address-family ipv4 4453 neighbors

EIGRP-IPv4 VR(Virtual-name) Address-family Neighbors for AS(4453)
Address          Interface    Hold Uptime  SRTT  RTO    Q      Seq
                (sec)      (ms)  (ms)  (ms)   Cnt    Num
172.16.81.28     Ethernet1   13   0:00:41  0     11    4    20
172.16.80.28     Ethernet0   14   0:02:01  0     10    12   24
172.16.80.31     Ethernet0   12   0:02:02  0     4     5    20
```

[Table 75](#) describes the significant fields shown in the display.

The following example shows how to display detailed information about neighbors that are discovered by EIGRP, including whether a neighbor has been gracefully restarted:

```
Router# show eigrp address-family ipv4 neighbors detail

EIGRP-IPv4 VR(test) Address-Family Neighbors for AS(3)
H Address Interface Hold Uptime SRTT RTO Q Seq
          (sec)      (ms)  (ms)  (ms)  Cnt  Num
172.16.81.28 Et1/1 11 01:11:08 10 200 0 8
Time since Restart 00:00:05
Version 5.0/3.0, Retrans: 2, Retries: 0, Prefixes: 2
Topology-ids from peer - 0
```

Table 75 *show eigrp address-family neighbors Field Descriptions*

| Field | Description |
|--------------------|---|
| AS(4453) | Autonomous system number specified in the configuration command, in this example 4453. |
| Address | IP address of the peer. |
| Interface | Interface on which the router is receiving hello packets from the peer. |
| Hold time | Length of time, in seconds, that the router will wait to hear from the peer before declaring it down. If the peer is using the default hold time, this number will be less than 15. If the peer configures a nondefault hold time, it will be reflected here. |
| Uptime | Elapsed time since the local router first heard from this neighbor. |
| Q Cnt | Number of packets (update, query, and reply) that the software is waiting to send. |
| Seq Num | Sequence number of the last update, query, or reply packet that was received from this neighbor. |
| SRTT | Smooth round-trip time. This is the number of milliseconds that it takes for an EIGRP packet to be sent to this neighbor and for the local router to receive an acknowledgment of that packet. |
| RTO | Retransmission timeout, in milliseconds. Indicates the amount of time EIGRP waits before retransmitting a packet from the retransmission queue to a neighbor. |
| Time since Restart | Time elapsed since a neighbor has been gracefully restarted. |

■ show eigrp address-family neighbors

| Related Commands | Command | Description |
|------------------|---|---|
| | show eigrp address-family accounting | Displays prefix accounting information for EIGRP processes. |
| | show eigrp address-family events | Displays information about EIGRP events. |
| | show eigrp address-family interfaces | Displays information about interfaces configured for EIGRP. |
| | show eigrp address-family sia-event | Displays information about EIGRP SIA events. |
| | show eigrp address-family sia-statistics | Displays information about EIGRP SIA statistics. |
| | show eigrp address-family timers | Displays information about EIGRP timers and expiration times. |
| | show eigrp address-family topology | Displays entries in the EIGRP topology table. |
| | show eigrp address-family traffic | Displays the number of EIGRP packets sent and received. |

show eigrp address-family timers

To display information about Enhanced Interior Gateway Routing Protocol (EIGRP) timers and expiration times, use the **show eigrp address-family timers** command in user EXEC or privileged EXEC mode.

```
show eigrp address-family {ipv4 | ipv6} [vrf vrf-name] [autonomous-system-number] [multicast]
timers
```

| Syntax Description | | |
|---------------------------------|--|--|
| ipv4 | Selects the IPv4 protocol address family. | |
| ipv6 | Selects the IPv6 protocol address family. | |
| vrf <i>vrf-name</i> | (Optional) Displays information about the specified VRF. | |
| <i>autonomous-system-number</i> | (Optional) Autonomous system number. | |
| multicast | (Optional) Displays information about multicast instances. | |

Command Default Information about all EIGRP timers is displayed.

Command Modes User EXEC (>)
Privileged EXEC (#)

| Command History | Release | Modification |
|-----------------|--------------------------|---|
| | 15.0(1)M | This command was introduced. |
| | 12.2(33)SRE | This command was integrated into Cisco IOS Release 12.2(33)SRE. |
| | 12.2(33)XNE | This command was integrated into Cisco IOS Release 12.2(33)XNE. |
| | Cisco IOS XE Release 2.5 | This command was integrated into Cisco IOS XE Release 2.5. |

Usage Guidelines This command is useful for debugging and troubleshooting by Cisco technical support, but it is not intended for normal EIGRP administration tasks. This command should not be used without guidance from Cisco technical support.

This command can be used to display information about EIGRP named configurations and EIGRP autonomous-system (AS) configurations.

This command displays the same information as the **show ip eigrp timers** command. Cisco recommends using the **show eigrp address-family timers** command.

Examples The following example shows how to display information about EIGRP timers:

```
Router# show eigrp address-family ipv4 4453 timers
```

```
EIGRP-IPv4 VR(Virtual-name) Address-family Timers for AS(4453)
```

■ **show eigrp address-family timers**

```

Hello Process
Expiration Type
| 1.022 (parent)
| 1.022 Hello (Et0/0)

Update Process
Expiration Type
| 14.984 (parent)
| 14.984 (parent)
| 14.984 Peer holding

SIA Process
Expiration Type for Topo(base)
| 0.000 (parent)

```

Related Commands

| Command | Description |
|---|---|
| show eigrp address-family accounting | Displays prefix accounting information for EIGRP processes. |
| show eigrp address-family events | Displays information about EIGRP events. |
| show eigrp address-family interfaces | Displays information about interfaces configured for EIGRP. |
| show eigrp address-family neighbors | Displays the neighbors discovered by EIGRP. |
| show eigrp address-family sia-event | Displays information about EIGRP SIA events. |
| show eigrp address-family sia-statistics | Displays information about EIGRP SIA statistics. |
| show eigrp address-family topology | Displays entries in the EIGRP topology table. |
| show eigrp address-family traffic | Displays the number of EIGRP packets sent and received. |

show eigrp address-family topology

To display entries in the Enhanced Interior Gateway Routing Protocol (EIGRP) topology table, use the **show eigrp address-family topology** command in user EXEC or privileged EXEC mode.

```
show eigrp address-family { ipv4 | ipv6 } [vrf vrf-name] [autonomous-system-number] [multicast]
topology [topology-name] [ip-address] [active] [all-links] [detail-links] [pending]
[summary] [zero-successors] [route-type { connected | external | internal | local |
redistributed | summary | vpn}]
```

Syntax Description

| | |
|---------------------------------|---|
| ipv4 | Selects the IPv4 protocol address family. |
| ipv6 | Selects the IPv6 protocol address family. |
| vrf <i>vrf-name</i> | (Optional) Displays information about the specified VRF. |
| <i>autonomous-system-number</i> | (Optional) Specifies the autonomous system number. |
| multicast | (Optional) Displays information about multicast instances. |
| <i>topology-name</i> | (Optional) Named entry in the EIGRP topology table. |
| <i>ip-address</i> | (Optional) Network or network and mask. When specified, a detailed description of the entry is provided. |
| active | (Optional) Displays only active entries in the EIGRP topology table. |
| all-links | (Optional) Displays all entries in the EIGRP topology table (including non-feasible-successor sources). |
| detail-links | (Optional) Displays detailed information about all entries in the topology table. |
| pending | (Optional) Displays all entries in the EIGRP topology table that are waiting for an update from a neighbor or are waiting to reply to a neighbor. |
| summary | (Optional) Displays summary information about the EIGRP topology table. |
| zero-successors | (Optional) Displays available routes in the EIGRP topology table that have zero successors. |
| route-type | (Optional) Displays information about services of the specified route type. |
| connected | (Optional) Displays information about all connected routes. |
| external | (Optional) Displays information about all external routes. |
| internal | (Optional) Displays information about all internal routes. |
| local | (Optional) Displays information about all locally originated routes. |
| redistributed | (Optional) Displays information about all redistributed routes. |
| summary | (Optional) Displays information about all summary routes. |
| vpn | (Optional) Displays information about all VPN sourced routes. Applies to IPv4 only. |

Command Default

If this command is used without any keywords or arguments, only routes that are feasible successors are displayed.

show eigrp address-family topology

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

| Release | Modification |
|--------------------------|---|
| 15.0(1)M | This command was introduced. |
| 12.2(33)SRE | This command was integrated into Cisco IOS Release 12.2(33)SRE. |
| 12.2(33)XNE | This command was integrated into Cisco IOS Release 12.2(33)XNE. |
| Cisco IOS XE Release 2.5 | This command was integrated into Cisco IOS XE Release 2.5. |

Usage Guidelines

This command can be used to display information about EIGRP named configurations and EIGRP autonomous-system (AS) configurations.

This command displays the same information as the **show ip eigrp topology** command. Cisco recommends using the **show eigrp address-family topology** command.

Examples

The following example shows how to display entries in the EIGRP topology table:

```
Router# show eigrp address-family ipv4 4453 topology

EIGRP-IPv4 VR(Virtual-name) Topology Table for AS(4453)/ID(10.0.0.1)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - Reply status, s - sia Status
P 10.17.17.0/24, 1 successors, FD is 409600
   via 10.10.10.2 (409600/128256), Ethernet3/0
P 172.16.19.0/24, 1 successors, FD is 409600
   via 10.10.10.2 (409600/128256), Ethernet3/0
P 192.168.10.0/24, 1 successors, FD is 281600
   via Connected, Ethernet3/0
P 10.10.10.0/24, 1 successors, FD is 281600
   via Redistributed (281600/0)
```

The following example shows how to display EIGRP metrics for specified internal services and external services:

```
Router# show eigrp address-family ipv4 4453 topology 10.10.10.0/24

EIGRP-IPv4 VR(virtual-name) Topology Entry for AS(4453)/ID(10.0.0.1) for 10.10.10.0/24
State is Passive, Query origin flag is 1, 1 Successor(s), FD is 128256
Descriptor Blocks:
0.0.0.0 (Null0), from Connected, Send flag is 0x0
Composite metric is (128256/0), service is Internal
Vector metric:
  Minimum bandwidth is 10000000 Kbit
  Total delay is 5000 microseconds
  Reliability is 255/255
  Load is 1/255
  Minimum MTU is 1514
  Hop count is 0
  Originating router is 10.0.0.1
```

Table 76 describes the significant fields shown in the display.

Table 76 *show eigrp address-family topology Field Descriptions*

| Field | Description |
|-----------------|--|
| Codes | State of this topology table entry. Passive and Active refer to the EIGRP state with respect to this destination; Update, Query, and Reply refer to the type of packet that is being sent. |
| P—Passive | No EIGRP computations are being performed for this destination. |
| A—Active | EIGRP computations are being performed for this destination. |
| U—Update | An update packet was sent to this destination. |
| Q—Query | A query packet was sent to this destination. |
| R—Reply | A reply packet was sent to this destination. |
| r—reply Status | Flag that is set after the software has sent a query and is waiting for a reply. |
| s—sia Status | Flag that is set if a route is in a stuck in active state. |
| successors | Number of successors. This number corresponds to the number of next hops in the IP routing table. If “successors” is capitalized, then the route or next hop is in a transition state. |
| FD | Feasible distance. The feasible distance is the best metric to reach the destination or the best metric that was known when the route went active. This value is used in the feasibility condition check. If the reported distance of the router (the metric after the slash) is less than the feasible distance, the feasibility condition is met and that path is a feasible successor. Once the software determines it has a feasible successor, it need not send a query for that destination. |
| replies | (Not shown in the output.) Number of replies that are still outstanding (have not been received) with respect to this destination. This information appears only when the destination is in the Active state. |
| state | (Not shown in the output) Exact EIGRP state that this destination is in. It can be the number 0, 1, 2, or 3. This information appears only when the destination is in the Active state. |
| via | IP address of the peer that told the software about this destination. The first N of these entries, where N is the number of successors, is the current successors. The remaining entries on the list are feasible successors. |
| (409600/128256) | The first number is the EIGRP metric that represents the cost to the destination. The second number is the EIGRP metric that this peer advertised. |
| Ethernet3/0 | Interface from which this information was learned. |

■ show eigrp address-family topology

| Related Commands | Command | Description |
|------------------|---|---|
| | show eigrp address-family accounting | Displays prefix accounting information for EIGRP processes. |
| | show eigrp address-family events | Displays information about EIGRP events. |
| | show eigrp address-family interfaces | Displays information about interfaces configured for EIGRP. |
| | show eigrp address-family neighbors | Displays the neighbors discovered by EIGRP. |
| | show eigrp address-family sia-event | Displays information about EIGRP SIA events. |
| | show eigrp address-family sia-statistics | Displays information about EIGRP SIA statistics. |
| | show eigrp address-family timers | Displays information about EIGRP timers and expiration times. |
| | show eigrp address-family traffic | Displays the number of EIGRP packets sent and received. |

show eigrp address-family traffic

To display the number of Enhanced Interior Gateway Routing Protocol (EIGRP) packets that are sent and received, use the **show eigrp address-family traffic** command in user EXEC or privileged EXEC mode.

```
show eigrp address-family { ipv4 | ipv6 } [vrf vrf-name] [autonomous-system-number] [multicast] traffic
```

| Syntax Description | | |
|---------------------------------|--|--|
| ipv4 | Selects the IPv4 protocol address family. | |
| ipv6 | Selects the IPv6 protocol address family. | |
| vrf <i>vrf-name</i> | (Optional) Displays information about the specified VRF. | |
| <i>autonomous-system-number</i> | (Optional) Autonomous system number. | |
| multicast | (Optional) Displays information about multicast instances. | |

Command Default The number of all EIGRP packets sent and received is displayed.

Command Modes User EXEC (>)
Privileged EXEC (#)

| Command History | Release | Modification |
|-----------------|--------------------------|---|
| | 15.0(1)M | This command was introduced. |
| | 12.2(33)SRE | This command was integrated into Cisco IOS Release 12.2(33)SRE. |
| | 12.2(33)XNE | This command was integrated into Cisco IOS Release 12.2(33)XNE. |
| | Cisco IOS XE Release 2.5 | This command was integrated into Cisco IOS XE Release 2.5. |

Usage Guidelines This command can be used to display information about EIGRP named configurations and EIGRP autonomous-system (AS) configurations.

This command displays the same information as the **show ip eigrp traffic** command. Cisco recommends using the **show eigrp address-family traffic** command.

Examples The following example shows how to display the number of EIGRP packets sent and received for autonomous system number 4453:

```
Router# show eigrp address-family ipv4 4453 traffic

EIGRP-IPv4 VR(virtual-name) Address-family Traffic Statistics for AS(4453)
  Hellos sent/received: 122/122
  Updates sent/received: 3/1
  Queries sent/received: 0/0
```


show eigrp address-family traffic

```

Replies sent/received: 0/0
Acks sent/received: 0/3
SIA-Queries sent/received: 0/0
SIA-Replies sent/received: 0/0
Hello Process ID: 128
PDM Process ID: 191
Socket Queue: 0/2000/1/0 (current/max/highest/drops)
Input Queue: 0/2000/1/0 (current/max/highest/drops)

```

Table 77 describes the significant fields shown in the display.

Table 77 *show eigrp address-family traffic Field Descriptions*

| Field | Description |
|---------------------------|--|
| Hellos sent/received | Number of hello packets sent and received. |
| Updates sent/received | Number of update packets sent and received. |
| Queries sent/received | Number of query packets sent and received. |
| Replies sent/received | Number of reply packets sent and received. |
| Acks sent/received | Number of acknowledgement packets sent and received. |
| SIA-Queries sent/received | Number of stuck in active query packets sent and received. |
| SIA-Replies sent/received | Number of stuck in active reply packets sent and received. |
| Hello Process ID | Cisco IOS hello process identifier. |
| PDM Process ID | Protocol-dependent module IOS process identifier. |
| Socket Queue | IP to EIGRP Hello Process socket queue counters. |
| Input Queue | EIGRP Hello Process to EIGRP PDM socket queue counters. |

Related Commands

| Command | Description |
|---|---|
| show eigrp address-family accounting | Displays prefix accounting information for EIGRP processes. |
| show eigrp address-family events | Displays information about EIGRP events. |
| show eigrp address-family interfaces | Displays information about interfaces configured for EIGRP. |
| show eigrp address-family neighbors | Displays the neighbors discovered by EIGRP. |
| show eigrp address-family sia-event | Displays information about EIGRP SIA events. |
| show eigrp address-family sia-statistics | Displays information about EIGRP SIA statistics. |
| show eigrp address-family timers | Displays information about EIGRP timers and expiration times. |
| show eigrp address-family topology | Displays entries in the EIGRP topology table. |

show erm statistics

To display the Embedded Resource Manager (ERM) Forwarding Information Base (FIB) ternary content addressable memory (TCAM) exception status for IPv4, IPv6, and Multiprotocol Label Switching (MPLS) protocols, use the **show erm statistics** command in privileged EXEC mode.

show erm statistics

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC

| Command History | Release | Modification |
|-----------------|--------------|---|
| | 12.2(17b)SXA | This command was introduced on the Supervisor Engine 720. |
| | 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |

Usage Guidelines This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

The IPv4, IPv6, and MPLS exception state displays FALSE when the protocol is not under the exception or displays TRUE when the protocol is under the exception.

Examples This example shows how to display FIB TCAM exception status for IPv4, IPv6, and MPLS protocols:

```
Router# show erm statistics

#IPv4 excep notified      = 0
#IPv6 excep notified      = 0
#MPLS excep notified      = 0
#IPv4 reloads done        = 0
#IPv6 reloads done        = 0
#MPLS reloads done        = 0
Current IPv4 excep state = FALSE
Current IPv6 excep state = FALSE
Current MPLS excep state = FALSE
#Timer expired            = 0
#of erm msgs               = 1
```

[Table 78](#) describes the significant fields shown in the display.

Table 78 *show erm statistics Field Descriptions*

| Field | Description |
|--|--|
| ... excep notified | The number of exceptions for each protocol. |
| ... reloads done | The number of reloads for each protocol. |
| ...Current <i>protocol</i> exception state | The current exception status of each protocol. |
| #of erm msgs | The number of ERM messages sent. |

Related Commands

| Command | Description |
|-------------------------|--|
| mls erm priority | Assigns the priorities to define an order in which protocols attempt to recover from the exception status. |

show fm ipv6 pbr all

To display IPv6 policy-based routing (PBR) value mask results (VMRs), use the **show fm ipv6 pbr all** command in privileged EXEC mode.

show fm ipv6 pbr all

Syntax Description This command has no arguments or keywords.

Command Default PBR configuration is not displayed.

Command Modes Privileged EXEC

| Command History | Release | Modification |
|------------------------|----------------|------------------------------|
| | 12.2(33)SX14 | This command was introduced. |

Usage Guidelines The **show fm ipv6 pbr all** command shows the IPv6 PBR VMRs for all interfaces with IPv6 PBR configured.

show fm ipv6 pbr interface

To displays the IPv6 policy-based routing (PBR) value mask results (VMRs) on a specified interface, use the **show fm ipv6 pbr interface** command in privileged EXEC mode.

```
show fm ipv6 pbr interface {interface type number}
```

| Syntax Description | interface type number Specified interface for which PBR VMR information will be displayed. | | | | |
|---------------------------|--|---------|--------------|--------------|------------------------------|
| Command Default | PBR VMR information on an interface is not displayed. | | | | |
| Command Modes | Privileged EXEC | | | | |
| Command History | <table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>12.2(33)SXI4</td> <td>This command was introduced.</td> </tr> </tbody> </table> | Release | Modification | 12.2(33)SXI4 | This command was introduced. |
| Release | Modification | | | | |
| 12.2(33)SXI4 | This command was introduced. | | | | |
| Usage Guidelines | The show fm ipv6 pbr all command shows the IPv6 PBR VMRs for a specified interface. | | | | |

show fm ipv6 traffic-filter

To display the IPv6 information, use the **show fm ipv6 traffic-filter** command in privileged EXEC mode.

```
show fm ipv6 traffic-filter {all | interface type number}
```

| Syntax Description | all | Displays IPv6 traffic filter information for all interfaces. |
|--------------------|------------------------------|--|
| | interface <i>type</i> | Displays IPv6 traffic filter information for the specified interface; possible valid values are ethernet , fastethernet , gigabitethernet , tengigabitethernet , pos , atm , ge-wan and vlan . |
| | <i>number</i> | Module and port number; see the "Usage Guidelines" section for valid values. |

Command Modes Privileged EXEC

| Command History | Release | Modification |
|-----------------|--------------|---|
| | 12.2(14)SX | This command was introduced on the Supervisor Engine 720. |
| | 12.2(17d)SXB | Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB. |
| | 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |

Usage Guidelines The **pos**, **atm**, and **ge-wan** keywords are supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

The *interface-number* argument designates the module and port number. Valid values for *interface-number* depend on the specified interface type and the chassis and module that are used. For example, if you specify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the module number are from 1 to 13 and valid values for the port number are from 1 to 48.

Examples This example shows how to display the IPv6 information for a specific interface:

```
Router# show fm ipv6 traffic-filter interface vlan 50
```

```
-----
FM_FEATURE_IPV6_ACG_INGRESS Name:testipv6 i/f: Vlan50
-----
DPort - Destination Port SPort - Source Port Pro - Protocol
X - XTAG TOS - TOS Value Res - VMR Result
RFM - R-Recirc. Flag MRTNP - M-Multicast Flag R - Reflexive flag
- F-Fragment flag - T-Tcp Control N - Non-cachable
- M-More Fragments - P-Mask Priority(H-High, L-Low)
Adj. - Adj. Index T - M(Mask)/V(Value) FM - Flow Mask
```

show fm ipv6 traffic-filter

NULL - Null FM SAO - Source Only FM DAO - Dest. Only FM
 SADA - Sour.& Dest. Only VSADA - Vlan SADA Only FF - Full Flow
 VFF - Vlan Full Flow F-VFF - Either FF or VFF A-VSD - Atleast VSADA
 A-FF - Atleast FF A-VFF - Atleast VFF A-SON - Atleast SAO
 A-DON - Atleast DAO A-SD - Atleast SADA SHORT - Shortest
 A-SFF - Any short than FF A-EFF - Any except FF A-EVFF- Any except VFF
 A-LVFF- Any less than VFF ERR - Flowmask Error

```

-----+-----+-----+-----+-----+
---+---+---+---+---+---+---+
|Indx|T| Dest IPv6 Addr | Source IPv6
Addr |Pro|RFM|X|MRTNP|Adj.| FM |
-----+-----+-----+-----+
---+---+---+---+---+---+
1 V 0:200E::
200D::1 0 -F- - ----L ---- Shorte
M 0:FFFF:FFFF:FFFF:FFFF::
FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF 0 1
TM_SOFT_BRIDGE_RESULT
2 V 0:200E::
200D::1 17 --- - ----L ---- Shorte
M 0:FFFF:FFFF:FFFF:FFFF::
FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF 255 0
TM_PERMIT_RESULT
3 V 200E::
200D::1 0 -F- - ----L ---- Shorte
M FFFF:FFFF:FFFF:FFFF:
FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF 0 1
TM_SOFT_BRIDGE_RESULT
4 V 200E::
200D::1 17 --- - ----L ---- Shorte
M FFFF:FFFF:FFFF:FFFF:
FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF 255 0
TM_PERMIT_RESULT
5 V
:: : 0 -F- - ----L ---- Shorte
M
:: : 0 1
TM_SOFT_BRIDGE_RESULT
6 V
:: : 0 -F- - ----L ---- Shorte
M
:: : 0 1
TM_SOFT_BRIDGE_RESULT
7 V
:: : 58 --- - ----L ---- Shorte
M
:: : 255 0
TM_PERMIT_RESULT
8 V
:: : 58 --- - ----L ---- Shorte
M
:: : 255 0
TM_PERMIT_RESULT
9 V
:: : 58 --- - ----L ---- Shorte
M
:: : 255 0

```

```

TM_PERMIT_RESULT
10 V
:: :: 58 --- - ----L ---- Shorte
M
:: :: 255 0
TM_PERMIT_RESULT
11 V
:: :: 58 --- - ----L ---- Shorte
M
:: :: 255 0
TM_PERMIT_RESULT
12 V
:: :: 58 --- - ----L ---- Shorte
M
:: :: 255 0
TM_PERMIT_RESULT
13 V
:: :: 58 --- - ----L ---- Shorte
M
:: :: 255 0
TM_PERMIT_RESULT
14 V
:: :: 58 --- - ----L ---- Shorte
M
:: :: 255 0
TM_PERMIT_RESULT
15 V
:: :: 0 --- - ----L ---- Shorte
M
:: :: 0 0
TM_L3_DENY_RESULT
Router#

```

This example shows how to display the IPv6 information for all interfaces:

```
Router# show fm ipv6 traffic-filter all
```

```

-----
FM_FEATURE_IPV6_ACG_INGRESS Name:testipv6 i/f: Vlan50
=====
DPort - Destination Port SPort - Source Port Pro - Protocol
X - XTAG TOS - TOS Value Res - VMR Result
RFM - R-Recirc. Flag MRTNP - M-Multicast Flag R - Reflexive flag
- F-Fragment flag - T-Tcp Control N - Non-cachable
- M-More Fragments - P-Mask Priority(H-High, L-Low)
Adj. - Adj. Index T - M(Mask)/V(Value) FM - Flow Mask
NULL - Null FM SAO - Source Only FM DAO - Dest. Only FM
SADA - Sour.& Dest. Only VSADA - Vlan SADA Only FF - Full Flow
VFF - Vlan Full Flow F-VFF - Either FF or VFF A-VSD - Atleast VSADA
A-FF - Atleast FF A-VFF - Atleast VFF A-SON - Atleast SAO
A-DON - Atleast DAO A-SD - Atleast SADA SHORT - Shortest
A-SFF - Any short than FF A-EFF - Any except FF A-EVFF- Any except VFF
A-LVFF- Any less than VFF ERR - Flowmask Error
+-----+-----+-----+-----+
---+---+---+---+---+---+

```


show fm ipv6 traffic-filter

```

|Indx|T| Dest IPv6 Addr | Source IPv6
Addr |Pro|RFM|X|MRTNP|Adj.| FM |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
-----+-----+-----+-----+-----+
1 V 0:200E::
200D::1 0 -F- - ----L ---- Shorte
M 0:FFFF:FFFF:FFFF:FFFF::
FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF 0 1
TM_SOFT_BRIDGE_RESULT
2 V 0:200E::
200D::1 17 --- - ----L ---- Shorte
M 0:FFFF:FFFF:FFFF:FFFF::
FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF 255 0
TM_PERMIT_RESULT
3 V 200E::
200D::1 0 -F- - ----L ---- Shorte
M FFFF:FFFF:FFFF:FFFF::
FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF 0 1
TM_SOFT_BRIDGE_RESULT
4 V 200E::
200D::1 17 --- - ----L ---- Shorte
M FFFF:FFFF:FFFF:FFFF::
FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF 255 0
TM_PERMIT_RESULT
5 V
:: : 0 -F- - ----L ---- Shorte
M
:: : 0 1
TM_SOFT_BRIDGE_RESULT
6 V
:: : 0 -F- - ----L ---- Shorte
M
:: : 0 1
TM_SOFT_BRIDGE_RESULT
7 V
:: : 58 --- - ----L ---- Shorte
M
:: : 255 0
TM_PERMIT_RESULT
8 V
:: : 58 --- - ----L ---- Shorte
M
:: : 255 0
TM_PERMIT_RESULT
9 V
:: : 58 --- - ----L ---- Shorte
M
:: : 255 0
TM_PERMIT_RESULT
10 V
:: : 58 --- - ----L ---- Shorte
M
:: : 255 0
13 V
:: : 58 --- - ----L ---- Shorte
M
:: : 255 0
.
. Output is truncated
.
Interface(s) using this IPv6 Ingress Traffic Filter:
V150,

```

show fm raguard

To display the interfaces configured with router advertisement (RA) guard, use the **show fm raguard** command in privileged EXEC mode.

show fm raguard

Syntax Description This command has no arguments or keywords.

Command Default RA guard interface information is not displayed.

Command Modes Privileged EXEC

Command History

| Release | Modification |
|--------------|--|
| 12.2(33)SX14 | This command was introduced. |
| 12.2(54)SG | This command was modified. Support for Cisco IOS Release 12.2(54)SG was added. |
| 12.2(50)SY | This command was integrated into Cisco IOS Release 12.2(50)SY. |

Usage Guidelines

Use the **show fm raguard** command to verify information about interfaces that are configured with RA guard.

Examples

The following example enables the display of interfaces configured with IPv6 RA guard:

```
Router# show fm raguard
```

```
-----
IPV6 RA GUARD in Ingress direction is configured on following interfaces
=====
Interface: Port-channel23
Interface: GigabitEthernet4/6
```

[Table 79](#) describes the significant fields shown in the display.

Table 79 *show fm raguard Field Descriptions*

| Field | Description |
|--|--|
| IPV6 RA GUARD in Ingress direction is configured on following interfaces | Displays the interfaces configured with IPv6 RA guard. |

show frame-relay lmi

To display statistics about the Local Management Interface (LMI), use the **show frame-relay lmi** command in user EXEC or privileged EXEC mode.

show frame-relay lmi [*type number*]

| Syntax Description | |
|--------------------|---|
| <i>type</i> | (Optional) Interface type; it must be serial . |
| <i>number</i> | (Optional) Interface number. |

| Command Modes | |
|---------------|-----------------|
| | User EXEC |
| | Privileged EXEC |

| Command History | Release | Modification |
|-----------------|-------------|---|
| | 10.0 | 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. |
| | 12.0(33)S | Support for IPv6 was added. This command was implemented on the Cisco 12000 series routers. |

Usage Guidelines Enter the command without arguments to obtain statistics about all Frame Relay interfaces.

Examples The following is sample output from the **show frame-relay lmi** command when the interface is a data terminal equipment (DTE) device:

```
Router# show frame-relay lmi

LMI Statistics for interface Serial1 (Frame Relay DTE) LMI TYPE = ANSI
  Invalid Unnumbered info 0          Invalid Prot Disc 0
  Invalid dummy Call Ref 0          Invalid Msg Type 0
  Invalid Status Message 0          Invalid Lock Shift 0
  Invalid Information ID 0          Invalid Report IE Len 0
  Invalid Report Request 0          Invalid Keep IE Len 0
  Num Status Eng. Sent 9            Num Status msgs Rcvd 0
  Num Update Status Rcvd 0          Num Status Timeouts 9
```

The following is sample output from the **show frame-relay lmi** command when the interface is a Network-to-Network Interface (NNI):

```
Router# show frame-relay lmi

LMI Statistics for interface Serial3 (Frame Relay NNI) LMI TYPE = CISCO
  Invalid Unnumbered info 0          Invalid Prot Disc 0
  Invalid dummy Call Ref 0          Invalid Msg Type 0
  Invalid Status Message 0          Invalid Lock Shift 0
```

```

Invalid Information ID 0
Invalid Report Request 0
Num Status Enq. Rcvd 11
Num Update Status Rcvd 0
Num Status Enq. Sent 10
Num Update Status Sent 0
Invalid Report IE Len 0
Invalid Keep IE Len 0
Num Status msgs Sent 11
Num St Enq. Timeouts 0
Num Status msgs Rcvd 10
Num Status Timeouts 0

```

Table 80 describes significant fields shown in the output.

Table 80 show frame-relay lmi Field Descriptions

| Field | Description |
|--------------------------|--|
| LMI Statistics | Signalling or LMI specification: CISCO, ANSI, or ITU-T. |
| Invalid Unnumbered info | Number of received LMI messages with invalid unnumbered information field. |
| Invalid Prot Disc | Number of received LMI messages with invalid protocol discriminator. |
| Invalid dummy Call Ref | Number of received LMI messages with invalid dummy call references. |
| Invalid Msg Type | Number of received LMI messages with invalid message type. |
| Invalid Status Message | Number of received LMI messages with invalid status message. |
| Invalid Lock Shift | Number of received LMI messages with invalid lock shift type. |
| Invalid Information ID | Number of received LMI messages with invalid information identifier. |
| Invalid Report IE Len | Number of received LMI messages with invalid Report IE Length. |
| Invalid Report Request | Number of received LMI messages with invalid Report Request. |
| Invalid Keep IE Len | Number of received LMI messages with invalid Keep IE Length. |
| Num Status Enq. Sent | Number of LMI status inquiry messages sent. |
| Num Status Msgs Rcvd | Number of LMI status messages received. |
| Num Update Status Rcvd | Number of LMI asynchronous update status messages received. |
| Num Status Timeouts | Number of times the status message was not received within the keepalive time value. |
| Num Status Enq. Rcvd | Number of LMI status enquiry messages received. |
| Num Status Msgs Sent | Number of LMI status messages sent. |
| Num Status Enq. Timeouts | Number of times the status enquiry message was not received within the T392 DCE timer value. |
| Num Update Status Sent | Number of LMI asynchronous update status messages sent. |

show frame-relay map

To display current Frame Relay map entries and information about connections, use the **show frame-relay map** command in privileged EXEC mode.

```
show frame-relay map [interface type number] [dlci]
```

| Syntax Description | |
|-------------------------------------|---|
| interface <i>type number</i> | (Optional) Specifies an interface for which mapping information will be displayed. A space is optional between the interface type and number. |
| <i>dlci</i> | (Optional) Specifies a data-link connection identifier (DLCI) for which mapping information will be displayed. Range: 16 to 1022. |

Command Default Static and dynamic Frame Relay map entries and information about connections for all DLCIs on all interfaces are displayed.

Command Modes Privileged EXEC

| Command History | Release | Modification |
|-----------------|--------------------------|---|
| | 10.0 | This command was introduced. |
| | 12.2(2)T | The display output for this command was modified to include the IPv6 address mappings of remote nodes to Frame Relay permanent virtual circuits (PVCs). |
| | 12.0(21)ST | This command was integrated into Cisco IOS Release 12.0(21)ST. |
| | 12.0(22)S | This command was integrated into Cisco IOS Release 12.0(22)S. |
| | 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |
| | 12.2(13)T | The display output for this command was modified to include information about Frame Relay PVC bundle maps. |
| | 12.2(28)SB | This command was integrated into Cisco IOS Release 12.2(28)SB, the interface keyword was added, and the <i>dlci</i> argument was added. |
| | 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| | 12.4(9)T | The interface keyword was added, and the <i>dlci</i> argument was 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. |
| | Cisco IOS XE Release 2.1 | This command was introduced on Cisco ASR 1000 Series Routers. |
| | 12.0(33)S | This command was implemented on the Cisco 12000 series routers. |

Examples This section contains the following examples:

- [Display All Maps or Maps for Specific DLCIs on Specific Interfaces or Subinterfaces: Example, page 1587](#)

- [Display Maps for PVC Bundles: Example, page 1588](#)
- [Display Maps for IPv6 Addresses: Example, page 1589](#)

Display All Maps or Maps for Specific DLCIs on Specific Interfaces or Subinterfaces: Example

The sample output in these examples uses the following configuration:

```
interface POS2/0
  no ip address
  encapsulation frame-relay
  frame-relay map ip 10.1.1.1 20 tcp header-compression
  frame-relay map ip 10.1.2.1 21 tcp header-compression
  frame-relay map ip 10.1.3.1 22 tcp header-compression
  frame-relay map bridge 23
  frame-relay interface-dlci 25
  frame-relay interface-dlci 26
  bridge-group 1
interface POS2/0.1 point-to-point
  frame-relay interface-dlci 24 protocol ip 10.1.4.1

interface Serial3/0
  no ip address
  encapsulation frame-relay
  serial restart-delay 0
  frame-relay map ip 172.16.3.1 20
  frame-relay map ip 172.16.4.1 21 tcp header-compression active
  frame-relay map ip 172.16.1.1 100
  frame-relay map ip 172.16.2.1 101
interface Serial3/0.1 multipoint
  frame-relay map ip 192.168.11.11 24
  frame-relay map ip 192.168.11.22 105
```

The following example shows how to display all maps:

Router# **show frame-relay map**

```
POS2/0 (up): ip 10.1.1.1 dlci 20(0x14,0x440), static,
             CISCO, status deleted
             TCP/IP Header Compression (enabled), connections: 256
POS2/0 (up): ip 10.1.2.1 dlci 21(0x15,0x450), static,
             CISCO, status deleted
             TCP/IP Header Compression (enabled), connections: 256
POS2/0 (up): ip 10.1.3.1 dlci 22(0x16,0x460), static,
             CISCO, status deleted
             TCP/IP Header Compression (enabled), connections: 256
POS2/0 (up): bridge dlci 23(0x17,0x470), static,
             CISCO, status deleted
POS2/0.1 (down): point-to-point dlci, dlci 24(0x18,0x480), broadcast
                status deleted
Serial3/0 (downup): ip 172.16.3.1 dlci 20(0x14,0x440), static,
                   CISCO, status deleted
Serial3/0 (downup): ip 172.16.4.1 dlci 21(0x15,0x450), static,
                   CISCO, status deleted
                   TCP/IP Header Compression (enabled), connections: 256
Serial3/0.1 (downup): ip 192.168.11.11 dlci 24(0x18,0x480), static,
                     CISCO, status deleted
Serial3/0 (downup): ip 172.16.1.1 dlci 100(0x64,0x1840), static,
                   CISCO, status deleted
Serial3/0 (downup): ip 172.16.2.1 dlci 101(0x65,0x1850), static,, CISCO,
                   CISCO, status deleted
                   ECRTP Header Compression (enabled, IETF), connections 16
                   TCP/IP Header Compression (enabled, IETF), connections 16
Serial3/0.1 (downup): ip 192.168.11.22 dlci 105(0x69,0x1890), static,
                    CISCO, status deleted
```

show frame-relay map

```
Serial4/0/1:0.1 (up): point-to-point dlci, dlci 102(0x66,0x1860), broadcast, CISCO
                    status defined, active,
                    RTP Header Compression (enabled), connections: 256
```

The following example shows how to display maps for a specific DLCI:

```
Router# show frame-relay map 20
```

```
POS2/0 (up): ip 10.1.1.1 dlci 20(0x14,0x440), static,
             CISCO, status deleted
             TCP/IP Header Compression (enabled), connections: 256
Serial3/0 (down): ip 172.16.3.1 dlci 20(0x14,0x440), static,
                CISCO, status deleted
```

The following example shows how to display maps for a specific interface:

```
Router# show frame-relay map interface pos2/0
```

```
POS2/0 (up): ip 10.1.1.1 dlci 20(0x14,0x440), static,
             CISCO, status deleted
             TCP/IP Header Compression (enabled), connections: 256
POS2/0 (up): ip 10.1.2.1 dlci 21(0x15,0x450), static,
             CISCO, status deleted
             TCP/IP Header Compression (enabled), connections: 256
POS2/0 (up): ip 10.1.3.1 dlci 22(0x16,0x460), static,
             CISCO, status deleted
             TCP/IP Header Compression (enabled), connections: 256
POS2/0 (up): bridge dlci 23(0x17,0x470), static,
             CISCO, status deleted
POS2/0.1 (down): point-to-point dlci, dlci 24(0x18,0x480), broadcast
                status deleted
```

The following example shows how to display maps for a specific DLCI on a specific interface:

```
Router# show frame-relay map interface pos2/0 20
```

```
POS2/0 (up): ip 10.1.1.1 dlci 20(0x14,0x440), static,
             CISCO, status deleted
             TCP/IP Header Compression (enabled), connections: 256
```

The following example shows how to display maps for a specific subinterface:

```
Router# show frame-relay map interface pos2/0.1
```

```
POS2/0.1 (down): point-to-point dlci, dlci 24(0x18,0x480), broadcast
                status deleted
```

The following example shows how to display maps for a specific DLCI on a specific subinterface:

```
Router# show frame-relay map interface pos2/0.1 24
```

```
POS2/0.1 (down): point-to-point dlci, dlci 24(0x18,0x480), broadcast
                status deleted
```

Display Maps for PVC Bundles: Example

The sample output in this example uses the following router configuration:

```
hostname router1
!
interface Serial2/0
 ip address 10.0.0.2 255.255.255.0
 encapsulation frame-relay
 frame-relay vc-bundle vcb1
  pvc 100 vcb1-classA
  precedence 1-7
```

```

class vcb1-classA
pvc 109 vcb1-others
precedence other
class others
frame-relay intf-type dce
!
map-class frame-relay vcb1-classA
frame-relay cir 128000
!
map-class frame-relay others
frame-relay cir 64000

hostname router2
!
interface Serial3/3
ip address 10.0.0.1 255.255.255.0
encapsulation frame-relay
frame-relay vc-bundle vcb1
pvc 100 vcb1-classA
precedence 1-7
class vcb1-classA
pvc 109 vcb1-others
precedence other
class others
!
map-class frame-relay vcb1-classA
frame-relay cir 128000
!
map-class frame-relay others
frame-relay cir 64000

```

The following sample output displays mapping information for two PVC bundles. The PVC bundle MAIN-1-static is configured with a static map. The map for PVC bundle MAIN-2-dynamic is created dynamically using Inverse Address Resolution Protocol (ARP).

```

Router# show frame-relay map

Serial1/4 (up): ip 10.1.1.1 vc-bundle MAIN-1-static, static,
                CISCO, status up
Serial1/4 (up): ip 10.1.1.2 vc-bundle MAIN-2-dynamic, dynamic,
                broadcast, status up

```

Display Maps for IPv6 Addresses: Example

The sample output in this example uses the following router configuration:

```

hostname router1
!
interface Serial2/0
no ip address
encapsulation frame-relay
!
interface Serial2/0.1 point-to-point
ipv6 address 1::1/64
frame-relay interface-dlci 101
!
interface Serial2/0.2 multipoint
ipv6 address 2::1/64
frame-relay map ipv6 2::2 201
frame-relay interface-dlci 201
!

hostname router2
!

```


■ show frame-relay map

```

interface Serial3/3
  no ip address
  encapsulation frame-relay
  frame-relay intf-type dce
  !
interface Serial3/3.1 point-to-point
  ipv6 address 1::2/64
  frame-relay interface-dlci 101
  !
interface Serial3/3.2 multipoint
  ipv6 address 2::2/64
  frame-relay map ipv6 3::1 201
  frame-relay interface-dlci 201
  !

```

The following sample output from the **show frame-relay map** command shows that the link-local and global IPv6 addresses (FE80::E0:F727:E400:A and 2001:0DB8:2222:1044::32; FE80::60:3E47:AC8:8 and 2001:0DB8:2222:1044::32) of two remote nodes are explicitly mapped to DLCI 17 and DLCI 19, respectively. Both DLCI 17 and DLCI 19 are terminated on interface serial 3 of this node; therefore, interface serial 3 of this node is a point-to-multipoint interface.

Router# **show frame-relay map**

```

Serial3 (up): ipv6 FE80::E0:F727:E400:A dlci 17(0x11,0x410), static,
              broadcast, CISCO, status defined, active
Serial3 (up): ipv6 2001:0DB8:2222:1044::32 dlci 19(0x13,0x430), static,
              CISCO, status defined, active

Serial3 (up): ipv6 2001:0DB8:2222:1044::32 dlci 17(0x11,0x410), static,
              CISCO, status defined, active
Serial3 (up): ipv6 FE80::60:3E47:AC8:8 dlci 19(0x13,0x430), static,
              broadcast, CISCO, status defined, active

```

[Table 81](#) describes the significant fields shown in the displays.

Table 81 show frame-relay map Field Descriptions

| Field | Description |
|---------------------|--|
| POS2/0 (up) | Identifies a Frame Relay interface and its status (up or down). |
| ip 10.1.1.1 | Destination IP address. |
| dlci 20(0x14,0x440) | DLCI that identifies the logical connection being used to reach this interface. This value is displayed in three ways: its decimal value (20), its hexadecimal value (0x14), and its value as it would appear on the wire (0x440). |
| vc-bundle | PVC bundle that serves as the logical connection being used to reach the interface. |
| static/dynamic | Indicates whether this is a static or dynamic entry. |
| broadcast | Indicates pseudobroadcasting. |
| CISCO | Indicates the encapsulation type for this map: either CISCO or IETF. |

Table 81 *show frame-relay map Field Descriptions (continued)*

| Field | Description |
|---|--|
| TCP/IP Header Compression (inherited), passive (inherited) | Indicates the header compression type (TCP/IP, Real-Time Transport Protocol (RTP), or Enhanced Compressed Real-Time Transport Protocol (ECRTP)) and whether the header compression characteristics were inherited from the interface or were explicitly configured for the IP map. |
| status defined, active | Indicates that the mapping between the destination address and the DLCI used to connect to the destination address is active. |

Related Commands

| Command | Description |
|-----------------------------------|---|
| show frame-relay pvc | Displays statistics about PVCs for Frame Relay interfaces. |
| show frame-relay vc-bundle | Displays attributes and other information about a Frame Relay PVC bundle. |

show frame-relay multilink

To display configuration information and statistics about multilink Frame Relay bundles and bundle links, use the **show frame-relay multilink** command in user EXEC or privileged EXEC mode.

```
show frame-relay multilink [mfr number | serial number] [dlci {dlci-number | lmi}] [detailed]
```

| Syntax Description | |
|----------------------|---|
| mfr number | (Optional) Displays information about a specific bundle interface. |
| serial number | (Optional) Displays information about a specific bundle link interface. |
| dlci | (Optional) Displays information about the data-link connection identifier (DLCI). |
| <i>dlci-number</i> | DLCI number. The range is from 16 to 1022. |
| lmi | Displays information about the Local Management Interface (LMI) DLCI. |
| detailed | (Optional) Displays more-detailed information, including counters for the control messages sent to and from the peer device and the status of the bundle links. |

Command Default Information for all bundles and bundle links is displayed.

Command Modes User EXEC (>)
Privileged EXEC (#)

| Command History | Release | Modification |
|-----------------|-------------|---|
| | 12.0(17)S | This command was introduced. |
| | 12.2(8)T | This command was integrated into Cisco IOS Release 12.2(8)T. |
| | 12.0(24)S | This command was implemented on VIP-enabled Cisco 7500 series routers. |
| | 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |
| | 12.3(4)T | This command was implemented on VIP-enabled Cisco 7500 series routers. |
| | 12.0(30)S | This command was updated to display Multilink Frame Relay variable bandwidth class status. |
| | 12.4(2)T | This command was updated to display Multilink Frame Relay variable bandwidth class status. |
| | 12.2(28)SB | This command was integrated into Cisco IOS Release 12.2(28)SB. |
| | 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| | 12.2SX | This command was integrated into 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. |
| | 12.0(33)S | Support for IPv6 was added. This command was implemented on the Cisco 12000 series routers. |

Examples**All Bundles and Bundle Links: Example**

The following is sample output from the **show frame-relay multilink** command (see [Table 82](#) for descriptions of the fields). Because a specific bundle or bundle link is not specified, information for all bundles and bundle links is displayed:

```
Router# show frame-relay multilink

Bundle:MFR0, State = up, class = A, fragmentation disabled
  BID = MFR0
  Bundle links :
    Serial2/1:3, HW state :up, Protocol state :Idle, LID :Serial2/1:3
    Serial2/1:2, HW state :up, Protocol state :Idle, LID :Serial2/1:2
    Serial2/1:1, HW state :up, Protocol state :Idle, LID :Serial2/1:1
```

The following is sample output from the **show frame-relay multilink** command when a Frame Relay bundle is configured as bandwidth class C (threshold) (see [Table 82](#) for descriptions of the fields):

```
Router# show frame-relay multilink

Bundle: MFR0, state down, class C (threshold 2), no fragmentation
  ID: bundle
  Serial5/1, state up/up, ID: bundle1
  Serial5/3, state up/add-sent, ID: bundle3
```

Bundle Link: Example

The following is sample output from the **show frame-relay multilink** command when it is entered with the **serial number** keyword and argument pair (see [Table 82](#) for descriptions of the fields). The example displays information about the specified bundle link:

```
Router# show frame-relay multilink serial 3/2

Bundle links :
  Serial3/2, HW state : down, Protocol state :Down_idle, LID :Serial3/2
  Bundle interface = MFR0, BID = MFR0
```

Detailed Bundle Links: Examples

The following is sample output from the **show frame-relay multilink** command when it is entered with the **serial number** keyword and argument pair and **detailed** keyword (see [Table 82](#) for descriptions of the fields). The example shows a bundle link in the “idle” state:

```
Router# show frame-relay multilink serial 3 detailed

Bundle links:

Serial3, HW state = up, link state = Idle, LID = Serial3
Bundle interface = MFR0, BID = MFR0
  Cause code = none, Ack timer = 4, Hello timer = 10,
  Max retry count = 2, Current count = 0,
  Peer LID = Serial5/3, RTT = 0 ms
  Statistics:
  Add_link sent = 0, Add_link rcv'd = 10,
  Add_link ack sent = 0, Add_link ack rcv'd = 0,
  Add_link rej sent = 10, Add_link rej rcv'd = 0,
  Remove_link sent = 0, Remove_link rcv'd = 0,
  Remove_link_ack sent = 0, Remove_link_ack rcv'd = 0,
  Hello sent = 0, Hello rcv'd = 0,
  Hello_ack sent = 0, Hello_ack rcv'd = 0,
  outgoing pak dropped = 0, incoming pak dropped = 0
```

The following is sample output from the **show frame-relay multilink** command when it is entered with the **serial number** keyword and argument pair and **detailed** keyword (see [Table 82](#) for descriptions of the fields). The example shows a bundle link in the “up” state:

```
Router# show frame-relay multilink serial 3 detailed

Bundle links:

Serial3, HW state = up, link state = Up, LID = Serial3
Bundle interface = MFR0, BID = MFR0
Cause code = none, Ack timer = 4, Hello timer = 10,
Max retry count = 2, Current count = 0,
Peer LID = Serial5/3, RTT = 4 ms
Statistics:
Add_link sent = 1, Add_link rcv'd = 20,
Add_link ack sent = 1, Add_link ack rcv'd = 1,
Add_link rej sent = 19, Add_link rej rcv'd = 0,
Remove_link sent = 0, Remove_link rcv'd = 0,
Remove_link_ack sent = 0, Remove_link_ack rcv'd = 0,
Hello sent = 0, Hello rcv'd = 1,
Hello_ack sent = 1, Hello_ack rcv'd = 0,
outgoing pak dropped = 0, incoming pak dropped = 0
```

[Table 82](#) describes significant fields shown in the displays.

Table 82 *show frame-relay multilink Field Descriptions*

| Field | Description |
|------------------|--|
| Bundle | Bundle interface. |
| State | Operational state of the bundle interface. |
| class | The bandwidth class criterion used to activate or deactivate a Frame Relay bundle. <ul style="list-style-type: none"> Class A (single link)—The bundle activates when any bundle link is up and deactivates when all bundle links are down (default). Class B (all links)—The bundle activates when all bundle links are up and deactivates when any bundle link is down. Class C (threshold)—The bundle activates when the minimum configured number of bundle links (the threshold) is up and deactivates when the minimum number of configured bundle links fails to meet the threshold. |
| BID | Bundle identification. |
| Bundle links | Bundle links for which information is displayed. |
| HW state | Operational state of the physical link. |
| Protocol state | Operational state of the bundle link line protocol. |
| link state | Operational state of the bundle link. |
| LID | Bundle link identification. |
| Bundle interface | Bundle interface with which the bundle link is associated. |

Table 82 *show frame-relay multilink Field Descriptions (continued)*

| Field | Description |
|--------------------|---|
| Cause code | <p>Can be one of the following values:</p> <ul style="list-style-type: none"> ack timer expiry—Add link synchronization process is exhausted. bundle link idle—Peer's bundle link is idle. This usually occurs when the peer's bundle interface is shut down. inconsistent bundle—Peer already has this bundle associated with another bundle. loopback detected—Local bundle link's physical line is looped back. none—ADD_LINK and ADD_LINK_ACK messages were properly exchanged, and no cause code was recorded. other—Indicates one of the following: a link identifier (LID) mismatch, an ID from the peer that is too long, or a failure to allocate ID memory. unexpected Add_link—ADD_LINK message is received when the bundle link is already in the "up" state. This code might appear when the line protocol is being set up, but will disappear once the connection is stabilized. |
| Ack timer | Number of seconds for which the bundle link waits for a hello acknowledgment before resending a hello message or resending an ADD_LINK message used for initial synchronization. |
| Hello timer | Interval at which a bundle link sends out hello messages. |
| Max retry count | Maximum number of times that a bundle link will resend a hello message before receiving an acknowledgment or resending an ADD_LINK message. |
| Current count | Number of retries that have been attempted. |
| Peer LID | Bundle link identification name of the peer end of the link. |
| RTT | Round-trip time (in milliseconds) as measured by using the Timestamp Information Element in the HELLO and HELLO_ACK messages. |
| Statistics | Displays statistics for each bundle link. |
| Add_link sent | Number of Add_link messages sent. Add_link messages notify the peer endpoint that the local endpoint is ready to process frames. |
| Add_link rcv'd | Number of Add_link messages received. |
| Add_link ack sent | Number of Add_link acknowledgments sent. Add_link acknowledgments notify the peer endpoint that an Add_link message was received. |
| Add_link ack rcv'd | Number of Add_link acknowledgments received. |
| Add_link rej sent | Number of Add_link_reject messages sent. |
| Add_link rej rcv'd | Number of Add_link_reject messages received. |

Table 82 *show frame-relay multilink Field Descriptions (continued)*

| Field | Description |
|-----------------------|---|
| Remove_link sent | Number of Remove_link messages sent. Remove_link messages notify the peer that on the local end a bundle link is being removed from the bundle. |
| Remove_link rcv'd | Number of Remove_link messages received. |
| Remove_link_ack sent | Number of Remove_link acknowledgments sent. Remove_link acknowledgments notify the peer that a Remove_link message has been received. |
| Remove_link_ack rcv'd | Number of Remove_link acknowledgments received. |
| Hello sent | Number of hello messages sent. Hello messages notify the peer endpoint that the local endpoint remains in the "up" state. |
| Hello rcv'd | Number of hello messages received. |
| Hello_ack sent | Number of hello acknowledgments sent. Hello acknowledgments notify the peer that hello messages have been received. |
| Hello_ack rcv'd | Number of hello acknowledgments received. |
| outgoing pak dropped | Number of outgoing packets dropped. |
| incoming pak dropped | Number of incoming packets dropped. |

Related Commands

| Command | Description |
|------------------------------------|---|
| debug frame-relay multilink | Displays debug messages for multilink Frame Relay bundles and bundle links. |

show frame-relay pvc

To display statistics about Frame Relay permanent virtual circuits (PVCs), use the **show frame-relay pvc** command in privileged EXEC mode.

```
show frame-relay pvc [[interface interface] [dcli] [64-bit] | summary [all]]
```

| Syntax Description | Parameter | Description |
|--------------------|------------------|--|
| | interface | (Optional) Specific interface for which PVC information will be displayed. |
| | <i>interface</i> | (Optional) Interface number containing the data-link connection identifiers (DLCIs) for which you wish to display PVC information. |
| | <i>dcli</i> | (Optional) A specific DLCI number used on the interface. Statistics for the specified PVC are displayed when a DLCI is also specified. |
| | 64-bit | (Optional) Displays 64-bit counter statistics. |
| | summary | (Optional) Displays a summary of all PVCs on the system. |
| | all | (Optional) Displays a summary of all PVCs on each interface. |

Command Modes Privileged EXEC

| Command History | Release | Modification |
|-----------------|-----------|--|
| | 10.0 | This command was introduced. |
| | 12.0(1)T | This command was modified to display statistics about virtual access interfaces used for PPP connections over Frame Relay. |
| | 12.0(3)XG | This command was modified to include the fragmentation type and size associated with a particular PVC when fragmentation is enabled on the PVC. |
| | 12.0(4)T | This command was modified to include the fragmentation type and size associated with a particular PVC when fragmentation is enabled on the PVC. |
| | 12.0(5)T | This command was modified to include information on the special voice queue that is created using the queue keyword of the frame-relay voice bandwidth command. |
| | 12.1(2)T | This command was modified to display the following information: <ul style="list-style-type: none"> • Details about the policy map attached to a specific PVC. • The priority configured for PVCs within Frame Relay PVC interface priority queueing. • Details about Frame Relay traffic shaping and policing on switched PVCs. |
| | 12.0(12)S | This command was modified to display reasons for packet drops and complete status information for switched NNI PVCs. |
| | 12.1(5)T | This command was modified to display the following information: <ul style="list-style-type: none"> • The number of packets in the post-hardware-compression queue. • The reasons for packet drops and complete status information for switched network-to-network PVCs. |

| Release | Modification |
|-------------|---|
| 12.0(17)S | This command was modified to display the number of outgoing packets dropped and the number of outgoing bytes dropped because of QoS policy. |
| 12.2 T | This command was modified to show that when payload compression is configured for a PVC, the throughput rate reported by the PVC is equal to the rate reported by the interface. |
| 12.2(4)T | The 64-bit keyword was added. |
| 12.2(11)T | This command was modified to display the number of outgoing packets dropped and the number of outgoing bytes dropped because of QoS policy. |
| 12.2(13)T | This command was modified to support display of Frame Relay PVC bundle information. |
| 12.2(15)T | This command was modified to support display of Frame Relay voice-adaptive fragmentation information. |
| 12.2(27)SBC | This command was integrated into Cisco IOS Release 12.2(27)SBC, and the summary and all keywords were added. |
| 12.2(28)SB | This command was integrated into Cisco IOS Release 12.2(28)SB, and support was added for hierarchical queueing framework (HQF). |
| 12.4(9)T | The summary and all keywords were added, and support was added for hierarchical queueing framework (HQF). |
| 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. |
| 12.0(33)S | Support for IPv6 was added. This command was implemented on the Cisco 12000 series routers. |

Usage Guidelines

Use this command to monitor the PPP link control protocol (LCP) state as being open with an up state or closed with a down state.

When “vofr” or “vofr cisco” has been configured on the PVC, and a voice bandwidth has been allocated to the class associated with this PVC, configured voice bandwidth and used voice bandwidth are also displayed.

Statistics Reporting

To obtain statistics about PVCs on all Frame Relay interfaces, use this command with no arguments.

To obtain statistics about a PVC that include policy-map configuration or the priority configured for that PVC, use this command with the *dcli* argument.

To display a summary of all PVCs on the system, use the **show frame-relay pvc** command with the **summary** keyword. To display a summary of all PVCs per interface, use the **summary all** keywords.

Per-VC counters are not incremented at all when either autonomous or silicon switching engine (SSE) switching is configured; therefore, PVC values will be inaccurate if either switching method is used.

You can change the period of time over which a set of data is used for computing load statistics. If you decrease the load interval, the average statistics are computed over a shorter period of time and are more responsive to bursts of traffic. To change the length of time for which a set of data is used to compute load statistics for a PVC, use the **load-interval** command in Frame-Relay DLCI configuration mode.

Traffic Shaping

Congestion control mechanisms are currently not supported on terminated PVCs nor on PVCs over ISDN. Where congestion control mechanisms are supported, the switch passes forward explicit congestion notification (FECN) bits, backward explicit congestion notification (BECN) bits, and discard eligible (DE) bits unchanged from entry points to exit points in the network.

Examples

The various displays in this section show sample output for a variety of PVCs. Some of the PVCs carry data only; some carry a combination of voice and data. This section contains the following examples:

- [Summary of Frame Relay PVCs: Example, page 1599](#)
- [Frame Relay Generic Configuration: Example, page 1600](#)
- [Frame Relay Voice-Adaptive Fragmentation: Example, page 1600](#)
- [Frame Relay PVC Bundle: Example, page 1600](#)
- [Frame Relay 64-Bit Counter: Example, page 1601](#)
- [Frame Relay Fragmentation and Hardware Compression: Example, page 1601](#)
- [Switched PVC: Example, page 1601](#)
- [Frame Relay Congestion Management on a Switched PVC: Example, page 1602](#)
- [Frame Relay Policing on a Switched PVC: Example, page 1602](#)
- [Frame Relay PVC Priority Queueing: Example, page 1603](#)
- [Low Latency Queueing for Frame Relay: Example, page 1603](#)
- [PPP over Frame Relay: Example, page 1604](#)
- [Voice over Frame Relay: Example, page 1604](#)
- [FRF.12 Fragmentation: Example, page 1605](#)
- [Multipoint Subinterfaces Transporting Data: Example, page 1605](#)
- [PVC Shaping When HQF is Enabled: Example, page 1606](#)
- [PVC Transporting Voice and Data: Example, page 1606](#)

Summary of Frame Relay PVCs: Example

The following example shows sample output of the **show frame-relay pvc** command with the **summary** keyword. The **summary** keyword displays all PVCs on the system.

```
Router# show frame-relay pvc summary
```

```
Frame-Relay VC Summary
```

| | Active | Inactive | Deleted | Static |
|----------|--------|----------|---------|--------|
| Local | 0 | 12 | 0 | 0 |
| Switched | 0 | 0 | 0 | 0 |
| Unused | 0 | 0 | 0 | 0 |

The following example shows sample output for the **show frame-relay pvc** command with the **summary** and **all** keywords. The **summary** and **all** keywords display all PVCs per interface.

```
Router# show frame-relay pvc summary all
```

```
VC Summary for interface Serial3/0 (Frame Relay DTE)
```

show frame-relay pvc

| | Active | Inactive | Deleted | Static |
|----------|--------|----------|---------|--------|
| Local | 0 | 7 | 0 | 0 |
| Switched | 0 | 0 | 0 | 0 |
| Unused | 0 | 0 | 0 | 0 |

VC Summary for interface Serial3/1 (Frame Relay DTE)

| | Active | Inactive | Deleted | Static |
|----------|--------|----------|---------|--------|
| Local | 0 | 5 | 0 | 0 |
| Switched | 0 | 0 | 0 | 0 |
| Unused | 0 | 0 | 0 | 0 |

Frame Relay Generic Configuration: Example

The following sample output shows a generic Frame Relay configuration on DLCI 100:

```
Router# show frame-relay pvc 100
```

PVC Statistics for interface Serial4/0/1:0 (Frame Relay DTE)

DLCI = 100, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE (EEK UP), INTERFACE = Serial4/0/1:0.1

```
input pkts 4360          output pkts 4361          in bytes 146364
out bytes 130252        dropped pkts 3735        in pkts dropped 0
out pkts dropped 3735    out bytes dropped 1919790
late-dropped out pkts 3735    late-dropped out bytes 1919790
in FECN pkts 0          in BECN pkts 0          out FECN pkts 0
out BECN pkts 0          in DE pkts 0            out DE pkts 0
out bcast pkts 337      out bcast bytes 102084
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
pvc create time 05:34:06, last time pvc status changed 05:33:38
```

Frame Relay Voice-Adaptive Fragmentation: Example

The following sample output indicates that Frame Relay voice-adaptive fragmentation is active on DLCI 202 and there are 29 seconds left on the deactivation timer. If no voice packets are detected in the next 29 seconds, Frame Relay voice-adaptive fragmentation will become inactive.

```
Router# show frame-relay pvc 202
```

PVC Statistics for interface Serial3/1 (Frame Relay DTE)

DLCI = 202, DLCI USAGE = LOCAL, PVC STATUS = STATIC, INTERFACE = Serial3/1.2

```
input pkts 0            output pkts 479          in bytes 0
out bytes 51226        dropped pkts 0           in pkts dropped 0
out pkts dropped 0      out bytes dropped 0
in FECN pkts 0          in BECN pkts 0          out FECN pkts 0
out BECN pkts 0          in DE pkts 0            out DE pkts 0
out bcast pkts 0        out bcast bytes 0
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 5000 bits/sec, 5 packets/sec
pvc create time 00:23:36, last time pvc status changed 00:23:31
fragment type end-to-end fragment size 80 adaptive active, time left 29 secs
```

Frame Relay PVC Bundle: Example

The following sample output indicates that PVC 202 is a member of VC bundle MAIN-1-static:

```
Router# show frame-relay pvc 202
```

PVC Statistics for interface Serial1/4 (Frame Relay DTE)

DLCI = 202, DLCI USAGE = LOCAL, PVC STATUS = STATIC, INTERFACE = Serial1/4

```

input pkts 0          output pkts 45          in bytes 0
out bytes 45000       dropped pkts 0          in FECN pkts 0
in BECN pkts 0       out FECN pkts 0        out BECN pkts 0
in DE pkts 0          out DE pkts 0
out bcast pkts 0     out bcast bytes 0
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 2000 bits/sec, 2 packets/sec
pvc create time 00:01:25, last time pvc status changed 00:01:11
VC-Bundle MAIN-1-static

```

Frame Relay 64-Bit Counter: Example

The following sample output displays the Frame Relay 64-bit counters:

```
Router# show frame-relay pvc 35 64-bit
```

```

DLCI = 35, INTERFACE = Serial0/0
input pkts 0          output pkts 0
in bytes 0            out bytes 0

```

Frame Relay Fragmentation and Hardware Compression: Example

The following is sample output for the **show frame-relay pvc** command for a PVC configured with Cisco-proprietary fragmentation and hardware compression:

```
Router# show frame-relay pvc 110
```

```
PVC Statistics for interface Serial0/0 (Frame Relay DTE)
```

```
DLCI = 110, DLCI USAGE = LOCAL, PVC STATUS = STATIC, INTERFACE = Serial0/0
```

```

input pkts 409          output pkts 409          in bytes 3752
out bytes 4560          dropped pkts 1           in FECN pkts 0
in BECN pkts 0          out FECN pkts 0         out BECN pkts 0
in DE pkts 0            out DE pkts 0
out bcast pkts 0        out bcast bytes 0
pvc create time 3d00h, last time pvc status changed 2d22h
Service type VoFR-cisco
Voice Queueing Stats: 0/100/0 (size/max/dropped)
Post h/w compression queue: 0
Current fair queue configuration:
  Discard    Dynamic    Reserved
  threshold  queue count  queue count
  64         16          2
Output queue size 0/max total 600/drops 0
configured voice bandwidth 16000, used voice bandwidth 0
fragment type VoFR-cisco          fragment size 100
cir 64000    bc 640    be 0    limit 80    interval 10
mincir 32000  byte increment 80    BECN response no
frags 428    bytes 4810    frags delayed 24    bytes delayed 770
shaping inactive
traffic shaping drops 0
ip rtp priority parameters 16000 32000 20000

```

Switched PVC: Example

The following is sample output from the **show frame-relay pvc** command for a switched Frame Relay PVC. This output displays detailed information about Network-to-Network Interface (NNI) status and why packets were dropped from switched PVCs.

```
Router# show frame-relay pvc
```

```
PVC Statistics for interface Serial2/2 (Frame Relay NNI)
```

show frame-relay pvc

```
DLCI = 16, DLCI USAGE = SWITCHED, PVC STATUS = INACTIVE, INTERFACE = Serial2/2
LOCAL PVC STATUS = INACTIVE, NNI PVC STATUS = INACTIVE
```

```
input pkts 0          output pkts 0          in bytes 0
out bytes 0          dropped pkts 0        in FECN pkts 0
in BECN pkts 0      out FECN pkts 0      out BECN pkts 0
in DE pkts 0        out DE pkts 0
out bcast pkts 0    out bcast bytes 0
switched pkts0
Detailed packet drop counters:
no out intf 0      out intf down 0      no out PVC 0
in PVC down 0     out PVC down 0      pkt too big 0
shaping Q full 0  pkt above DE 0      policing drop 0
pvc create time 00:00:07, last time pvc status changed 00:00:07
```

Frame Relay Congestion Management on a Switched PVC: Example

The following is sample output from the **show frame-relay pvc** command that shows the statistics for a switched PVC on which Frame Relay congestion management is configured:

```
Router# show frame-relay pvc 200
```

```
PVC Statistics for interface Serial3/0 (Frame Relay DTE)
```

```
DLCI = 200, DLCI USAGE = SWITCHED, PVC STATUS = ACTIVE, INTERFACE = Serial3/0
```

```
input pkts 341      output pkts 390      in bytes 341000
out bytes 390000    dropped pkts 0       in FECN pkts 0
in BECN pkts 0     out FECN pkts 0     out BECN pkts 0
in DE pkts 0       out DE pkts 390
out bcast pkts 0   out bcast bytes 0    Num Pkts Switched 341
```

```
pvc create time 00:10:35, last time pvc status changed 00:10:06
Congestion DE threshold 50
shaping active
cir 56000    bc 7000    be 0    byte limit 875    interval 125
mincir 28000    byte increment 875    BECN response no
pkts 346    bytes 346000    pkts delayed 339    bytes delayed 339000
traffic shaping drops 0
Queueing strategy:fifo
Output queue 48/100, 0 drop, 339 dequeued
```

Frame Relay Policing on a Switched PVC: Example

The following is sample output from the **show frame-relay pvc** command that shows the statistics for a switched PVC on which Frame Relay policing is configured:

```
Router# show frame-relay pvc 100
```

```
PVC Statistics for interface Serial1/0 (Frame Relay DCE)
```

```
DLCI = 100, DLCI USAGE = SWITCHED, PVC STATUS = ACTIVE, INTERFACE = Serial1/0
```

```
input pkts 1260      output pkts 0          in bytes 1260000
out bytes 0          dropped pkts 0        in FECN pkts 0
in BECN pkts 0      out FECN pkts 0      out BECN pkts 0
in DE pkts 0        out DE pkts 0
out bcast pkts 0    out bcast bytes 0    Num Pkts Switched 1260
```

```
pvc create time 00:03:57, last time pvc status changed 00:03:19
policing enabled, 180 pkts marked DE
policing Bc 6000    policing Be 6000    policing Tc 125 (msec)
in Bc pkts 1080    in Be pkts 180    in xs pkts 0
in Bc bytes 1080000    in Be bytes 180000    in xs bytes 0
```

Frame Relay PVC Priority Queueing: Example

The following is sample output for a PVC that has been assigned high priority:

```
Router# show frame-relay pvc 100

PVC Statistics for interface Serial0 (Frame Relay DTE)

DLCI = 100, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = Serial0

  input pkts 0          output pkts 0          in bytes 0
  out bytes 0          dropped pkts 0          in FECN pkts 0
  in BECN pkts 0        out FECN pkts 0        out BECN pkts 0
  in DE pkts 0          out DE pkts 0
  out bcast pkts 0      out bcast bytes 0
pvc create time 00:00:59, last time pvc status changed 00:00:33
priority high
```

Low Latency Queueing for Frame Relay: Example

The following is sample output from the **show frame-relay pvc** command for a PVC shaped to a 64000 bps committed information rate (CIR) with fragmentation. A policy map is attached to the PVC and is configured with a priority class for voice, two data classes for IP precedence traffic, and a default class for best-effort traffic. Weighted Random Early Detection (WRED) is used as the drop policy on one of the data classes.

```
Router# show frame-relay pvc 100

PVC Statistics for interface Serial1/0 (Frame Relay DTE)

DLCI = 100, DLCI USAGE = LOCAL, PVC STATUS = INACTIVE, INTERFACE = Serial1/0.1

  input pkts 0          output pkts 0          in bytes 0
  out bytes 0          dropped pkts 0          in FECN pkts 0
  in BECN pkts 0        out FECN pkts 0        out BECN pkts 0
  in DE pkts 0          out DE pkts 0
  out bcast pkts 0      out bcast bytes 0
pvc create time 00:00:42, last time pvc status changed 00:00:42
service policy mypolicy
Class voice
  Weighted Fair Queueing
    Strict Priority
    Output Queue: Conversation 72
    Bandwidth 16 (kbps) Packets Matched 0
    (pkts discards/bytes discards) 0/0
Class immediate-data
  Weighted Fair Queueing
    Output Queue: Conversation 73
    Bandwidth 60 (%) Packets Matched 0
    (pkts discards/bytes discards/tail drops) 0/0/0
    mean queue depth: 0
    drops: class random tail min-th max-th mark-prob
           0 0 0 64 128 1/10
           1 0 0 71 128 1/10
           2 0 0 78 128 1/10
           3 0 0 85 128 1/10
           4 0 0 92 128 1/10
           5 0 0 99 128 1/10
           6 0 0 106 128 1/10
           7 0 0 113 128 1/10
           rsvp 0 0 120 128 1/10
Class priority-data
  Weighted Fair Queueing
    Output Queue: Conversation 74
```

show frame-relay pvc

```

Bandwidth 40 (%) Packets Matched 0 Max Threshold 64 (packets)
(pkts discards/bytes discards/tail drops) 0/0/0
Class class-default
  Weighted Fair Queueing
  Flow Based Fair Queueing
  Maximum Number of Hashed Queues 64 Max Threshold 20 (packets)
Output queue size 0/max total 600/drops 0
fragment type end-to-end      fragment size 50
cir 64000      bc      640      be 0      limit 80      interval 10
mincir 64000      byte increment 80      BECN response no
frags 0      bytes 0      frags delayed 0      bytes delayed 0
shaping inactive
traffic shaping drops 0

```

PPP over Frame Relay: Example

The following is sample output from the **show frame-relay pvc** command that shows the PVC statistics for serial interface 5 (slot 1 and DLCI 55 are up) during a PPP session over Frame Relay:

```
Router# show frame-relay pvc 55
```

```

PVC Statistics for interface Serial5/1 (Frame Relay DTE)
DLCI = 55, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = Serial5/1.1
  input pkts 9      output pkts 16      in bytes 154
  out bytes 338      dropped pkts 6      in FECN pkts 0
  in BECN pkts 0      out FECN pkts 0      out BECN pkts 0
  in DE pkts 0      out DE pkts 0
  out bcast pkts 0      out bcast bytes 0
  pvc create time 00:35:11, last time pvc status changed 00:00:22
  Bound to Virtual-Access1 (up, cloned from Virtual-Template5)

```

Voice over Frame Relay: Example

The following is sample output from the **show frame-relay pvc** command for a PVC carrying Voice over Frame Relay (VoFR) traffic configured via the **vofr cisco** command. The **frame-relay voice bandwidth** command has been configured on the class associated with this PVC, as has fragmentation. The fragmentation type employed is proprietary to Cisco.

A sample configuration for this situation is shown first, followed by the output for the **show frame-relay pvc** command.

```

interface serial 0
  encapsulation frame-relay
  frame-relay traffic-shaping
  frame-relay interface-dlci 108
  vofr cisco
  class vofr-class
map-class frame-relay vofr-class
  frame-relay fragment 100
  frame-relay fair-queue
  frame-relay cir 64000
  frame-relay voice bandwidth 25000

```

```
Router# show frame-relay pvc 108
```

```

PVC Statistics for interface Serial0 (Frame Relay DTE)
DLCI = 108, DLCI USAGE = LOCAL, PVC STATUS = STATIC, INTERFACE = Serial0
  input pkts 1260      output pkts 1271      in bytes 95671
  out bytes 98604      dropped pkts 0      in FECN pkts 0
  in BECN pkts 0      out FECN pkts 0      out BECN pkts 0
  in DE pkts 0      out DE pkts 0
  out bcast pkts 1271      out bcast bytes 98604
  pvc create time 09:43:17, last time pvc status changed 09:43:17
  Service type VoFR-cisco

```

```

configured voice bandwidth 25000, used voice bandwidth 0
voice reserved queues 24, 25
fragment type VoFR-cisco          fragment size 100
cir 64000      bc 64000      be 0          limit 1000  interval 125
mincir 32000   byte increment 1000 BECN response no
pkts 2592     bytes 205140   pkts delayed 1296     bytes delayed 102570
shaping inactive
shaping drops 0
Current fair queue configuration:
  Discard      Dynamic      Reserved
  threshold   queue count  queue count
    64         16         2
Output queue size 0/max total 600/drops 0

```

FRF.12 Fragmentation: Example

The following is sample output from the **show frame-relay pvc** command for an application employing pure FRF.12 fragmentation. A sample configuration for this situation is shown first, followed by the output for the **show frame-relay pvc** command.

```

interface serial 0
 encapsulation frame-relay
 frame-relay traffic-shaping
 frame-relay interface-dlci 110
 class frag
map-class frame-relay frag
 frame-relay fragment 100
 frame-relay fair-queue
 frame-relay cir 64000

```

Router# **show frame-relay pvc 110**

```

PVC Statistics for interface Serial0 (Frame Relay DTE)
DLCI = 110, DLCI USAGE = LOCAL, PVC STATUS = STATIC, INTERFACE = Serial0
  input pkts 0          output pkts 243        in bytes 0
  out bytes 7290       dropped pkts 0         in FECN pkts 0
  in BECN pkts 0      out FECN pkts 0       out BECN pkts 0
  in DE pkts 0        out DE pkts 0
  out bcast pkts 243   out bcast bytes 7290
pvc create time 04:03:17, last time pvc status changed 04:03:18
fragment type end-to-end          fragment size 100
cir 64000      bc 64000      be 0          limit 1000  interval 125
mincir 32000   byte increment 1000 BECN response no
pkts 486     bytes 14580   pkts delayed 243     bytes delayed 7290
shaping inactive
shaping drops 0
Current fair queue configuration:
  Discard      Dynamic      Reserved
  threshold   queue count  queue count
    64         16         2
Output queue size 0/max total 600/drops 0

```

Note that when voice is not configured, voice bandwidth output is not displayed.

Multipoint Subinterfaces Transporting Data: Example

The following is sample output from the **show frame-relay pvc** command for multipoint subinterfaces carrying data only. The output displays both the subinterface number and the DLCI. This display is the same whether the PVC is configured for static or dynamic addressing. Note that neither fragmentation nor voice is configured on this PVC.

show frame-relay pvc

Router# **show frame-relay pvc**

```

DLCI = 300, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = Serial0.103
input pkts 10  output pkts 7  in bytes 6222
out bytes 6034  dropped pkts 0  in FECN pkts 0
in BECN pkts 0  out FECN pkts 0  out BECN pkts 0
in DE pkts 0  out DE pkts 0
outbcast pkts 0  outbcast bytes 0
pvc create time 0:13:11  last time pvc status changed 0:11:46
DLCI = 400, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = Serial0.104
input pkts 20  output pkts 8  in bytes 5624
out bytes 5222  dropped pkts 0  in FECN pkts 0
in BECN pkts 0  out FECN pkts 0  out BECN pkts 0
in DE pkts 0  out DE pkts 0
outbcast pkts 0  outbcast bytes 0
pvc create time 0:03:57  last time pvc status changed 0:03:48

```

PVC Shaping When HQF is Enabled: Example

The following is sample output from the **show frame-relay pvc** command for a PVC when HQF is enabled:

Router# **show frame-relay pvc 16**

PVC Statistics for interface Serial4/1 (Frame Relay DTE)

```

DLCI = 16, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = Serial4/1

input pkts 1          output pkts 1          in bytes 34
out bytes 34          dropped pkts 0          in pkts dropped 0
out pkts dropped 0    out bytes dropped 0
in FECN pkts 0        in BECN pkts 0        out FECN pkts 0
out BECN pkts 0        in DE pkts 0          out DE pkts 0
out bcast pkts 1      out bcast bytes 34
pvc create time 00:09:07, last time pvc status changed 00:09:07
shaping inactive

```

PVC Transporting Voice and Data: Example

The following is sample output from the **show frame-relay pvc** command for a PVC carrying voice and data traffic, with a special queue specifically for voice traffic created using the **frame-relay voice bandwidth** command **queue** keyword:

Router# **show frame-relay pvc interface serial 1 45**

PVC Statistics for interface Serial11 (Frame Relay DTE)

DLCI = 45, DLCI USAGE = LOCAL, PVC STATUS = STATIC, INTERFACE = Serial11

```

input pkts 85          output pkts 289         in bytes 1730
out bytes 6580         dropped pkts 11         in FECN pkts 0
in BECN pkts 0        out FECN pkts 0        out BECN pkts 0
in DE pkts 0          out DE pkts 0
out bcast pkts 0      out bcast bytes 0
pvc create time 00:02:09, last time pvc status changed 00:02:09
Service type VoFR
configured voice bandwidth 25000, used voice bandwidth 22000
fragment type VoFR      fragment size 100
cir 20000  bc 1000  be 0  limit 125  interval 50
mincir 20000  byte increment 125  BECN response no
fragments 290  bytes 6613  fragments delayed 1  bytes delayed 33
shaping inactive
traffic shaping drops 0
Voice Queueing Stats: 0/100/0 (size/max/dropped)

```

```

~~~~~
Current fair queue configuration:
Discard      Dynamic      Reserved
threshold   queue count  queue count
64           16           2
Output queue size 0/max total 600/drops 0

```

Table 83 describes the significant fields shown in the displays.

Table 83 *show frame-relay pvc Field Descriptions*

| Field | Description |
|-------------------------------|--|
| DLCI | One of the DLCI numbers for the PVC. |
| DLCI USAGE | Lists SWITCHED when the router or access server is used as a switch, or LOCAL when the router or access server is used as a DTE device. |
| PVC STATUS | Status of the PVC: ACTIVE, INACTIVE, or DELETED. |
| INTERFACE | Specific subinterface associated with this DLCI. |
| LOCAL PVC STATUS ¹ | Status of PVC configured locally on the NNI interface. |
| NNI PVC STATUS ¹ | Status of PVC learned over the NNI link. |
| input pkts | Number of packets received on this PVC. |
| output pkts | Number of packets sent on this PVC. |
| in bytes | Number of bytes received on this PVC. |
| out bytes | Number of bytes sent on this PVC. |
| dropped pkts | Number of incoming and outgoing packets dropped by the router at the Frame Relay level. |
| in pkts dropped | Number of incoming packets dropped. Incoming packets may be dropped for a number of reasons, including the following: <ul style="list-style-type: none"> • Inactive PVC • Policing • Packets received above DE discard level • Dropped fragments • Memory allocation failures • Configuration problems |
| out pkts dropped | Number of outgoing packets dropped, including shaping drops and late drops. |
| out bytes dropped | Number of outgoing bytes dropped. |
| late-dropped out pkts | Number of outgoing packets dropped because of QoS policy (such as with VC queuing or Frame Relay traffic shaping). This field is not displayed when the value is zero. |
| late-dropped out bytes | Number of outgoing bytes dropped because of QoS policy (such as with VC queuing or Frame Relay traffic shaping). This field is not displayed when the value is zero. |
| in FECN pkts | Number of packets received with the FECN bit set. |
| in BECN pkts | Number of packets received with the BECN bit set. |

Table 83 show frame-relay pvc Field Descriptions (continued)

| Field | Description |
|------------------------------|--|
| out FECN pkts | Number of packets sent with the FECN bit set. |
| out BECN pkts | Number of packets sent with the BECN bit set. |
| in DE pkts | Number of DE packets received. |
| out DE pkts | Number of DE packets sent. |
| out bcast pkts | Number of output broadcast packets. |
| out bcast bytes | Number of output broadcast bytes. |
| switched pkts | Number of switched packets. |
| no out intf ² | Number of packets dropped because there is no output interface. |
| out intf down ² | Number of packets dropped because the output interface is down. |
| no out PVC ² | Number of packets dropped because the outgoing PVC is not configured. |
| in PVC down ² | Number of packets dropped because the incoming PVC is inactive. |
| out PVC down ² | Number of packets dropped because the outgoing PVC is inactive. |
| pkt too big ² | Number of packets dropped because the packet size is greater than media MTU ³ . |
| shaping Q full ² | Number of packets dropped because the Frame Relay traffic-shaping queue is full. |
| pkt above DE ² | Number of packets dropped because they are above the DE level when Frame Relay congestion management is enabled. |
| policing drop ² | Number of packets dropped because of Frame Relay traffic policing. |
| pvc create time | Time at which the PVC was created. |
| last time pvc status changed | Time at which the PVC changed status. |
| VC-Bundle | PVC bundle of which the PVC is a member. |
| priority | Priority assigned to the PVC. |
| pkts marked DE | Number of packets marked DE because they exceeded the Bc. |
| policing Bc | Committed burst size. |
| policing Be | Excess burst size. |
| policing Tc | Measurement interval for counting Bc and Be. |
| in Bc pkts | Number of packets received within the committed burst. |
| in Be pkts | Number of packets received within the excess burst. |
| in xs pkts | Number of packets dropped because they exceeded the combined burst. |
| in Bc bytes | Number of bytes received within the committed burst. |
| in Be bytes | Number of bytes received within the excess burst. |
| in xs bytes | Number of bytes dropped because they exceeded the combined burst. |
| Congestion DE threshold | PVC queue percentage at which packets with the DE bit are dropped. |
| Congestion ECN threshold | PVC queue percentage at which packets are set with the BECN and FECN bits. |

Table 83 show frame-relay pvc Field Descriptions (continued)

| Field | Description |
|---------------------------------|---|
| Service type | Type of service performed by this PVC. Can be VoFR or VoFR-cisco. |
| Post h/w compression queue | Number of packets in the post-hardware-compression queue when hardware compression and Frame Relay fragmentation are configured. |
| configured voice bandwidth | Amount of bandwidth in bits per second (bps) reserved for voice traffic on this PVC. |
| used voice bandwidth | Amount of bandwidth in bps currently being used for voice traffic. |
| service policy | Name of the output service policy applied to the VC. |
| Class | Class of traffic being displayed. Output is displayed for each configured class in the policy. |
| Output Queue | The WFQ ⁴ conversation to which this class of traffic is allocated. |
| Bandwidth | Bandwidth in kbps or percentage configured for this class. |
| Packets Matched | Number of packets that matched this class. |
| Max Threshold | Maximum queue size for this class when WRED is not used. |
| pkts discards | Number of packets discarded for this class. |
| bytes discards | Number of bytes discarded for this class. |
| tail drops | Number of packets discarded for this class because the queue was full. |
| mean queue depth | Average queue depth, based on the actual queue depth on the interface and the exponential weighting constant. It is a moving average. The minimum and maximum thresholds are compared against this value to determine drop decisions. |
| drops: | WRED parameters. |
| class | IP precedence value. |
| random | Number of packets randomly dropped when the mean queue depth is between the minimum threshold value and the maximum threshold value for the specified IP precedence value. |
| tail | Number of packets dropped when the mean queue depth is greater than the maximum threshold value for the specified IP precedence value. |
| min-th | Minimum WRED threshold in number of packets. |
| max-th | Maximum WRED threshold in number of packets. |
| mark-prob | Fraction of packets dropped when the average queue depth is at the maximum threshold. |
| Maximum Number of Hashed Queues | (Applies to class default only) Number of queues available for unclassified flows. |
| fragment type | Type of fragmentation configured for this PVC. Possible types are as follows: <ul style="list-style-type: none"> • end-to-end—Fragmented packets contain the standard FRF.12 header • VoFR—Fragmented packets contain the FRF.11 Annex C header • VoFR-cisco—Fragmented packets contain the Cisco proprietary header |
| fragment size | Size of the fragment payload in bytes. |

Table 83 show frame-relay pvc Field Descriptions (continued)

| Field | Description |
|--------------------------|--|
| adaptive active/inactive | Indicates whether Frame Relay voice-adaptive fragmentation is active or inactive. |
| time left | Number of seconds left on the Frame Relay voice-adaptive fragmentation deactivation timer. When this timer expires, Frame Relay fragmentation turns off. |
| cir | Current CIR in bps. |
| bc | Current committed burst (Bc) size, in bits. |
| be | Current excess burst (Be) size, in bits. |
| limit | Maximum number of bytes sent per internal interval (excess plus sustained). |
| interval | Interval being used internally (may be smaller than the interval derived from Bc/CIR; this happens when the router determines that traffic flow will be more stable with a smaller configured interval). |
| mincir | Minimum CIR for the PVC. |
| byte increment | Number of bytes that will be sustained per internal interval. |
| BECN response | Indication that Frame Relay has BECN adaptation configured. |
| pkts | Number of packets associated with this PVC that have gone through the traffic-shaping system. |
| frags | Total number of fragments (and unfragmented packets that are too small to be fragmented) shaped on this VC. |
| bytes | Number of bytes associated with this PVC that have gone through the traffic-shaping system. |
| pkts delayed | Number of packets associated with this PVC that have been delayed by the traffic-shaping system. |
| frags delayed | Number of fragments (and unfragmented packets that are too small to be fragmented) delayed in the shaping queue before being sent. |
| bytes delayed | Number of bytes associated with this PVC that have been delayed by the traffic-shaping system. |
| shaping | Indication that shaping will be active for all PVCs that are fragmenting data; otherwise, shaping will be active if the traffic being sent exceeds the CIR for this circuit. |
| shaping drops | Number of packets dropped by the traffic-shaping process. |
| Queueing strategy | Per-VC queueing strategy. |
| Output queue | State of the per-VC queue. |
| 48/100 | • Number of packets enqueued/size of the queue |
| 0 drop | • Number of packets dropped |
| 300 dequeued | • Number of packets dequeued |
| Voice Queueing Stats | Statistics showing the size of packets, the maximum number of packets, and the number of packets dropped in the special voice queue created using the frame-relay voice bandwidth command queue keyword. |

Table 83 show frame-relay pvc Field Descriptions (continued)

| Field | Description |
|----------------------|---|
| Discard threshold | Maximum number of packets that can be stored in each packet queue. Additional packets received after a queue is full will be discarded. |
| Dynamic queue count | Number of packet queues reserved for best-effort traffic. |
| Reserved queue count | Number of packet queues reserved for voice traffic. |
| Output queue size | Size in bytes of each output queue. |
| max total | Maximum number of packets of all types that can be queued in all queues. |
| drops | Number of frames dropped by all output queues. |

1. The LOCAL PVC STATUS and NNI PVC STATUS fields are displayed only for PVCs configured on Frame Relay NNI interface types. These fields are not displayed if the PVC is configured on DCE or DTE interface types.
2. The detailed packet drop fields are displayed for switched Frame Relay PVCs only. These fields are not displayed for terminated PVCs.
3. MTU = maximum transmission unit.
4. WFQ = weighted fair queueing.

Related Commands

| Command | Description |
|---|--|
| frame-relay accounting adjust | Enables byte count adjustment at the PVC level so that the number of bytes sent and received at the PVC corresponds to the actual number of bytes sent and received on the physical interface. |
| frame-relay interface-queue priority | Enables FR PIPQ on a Frame Relay interface and assigns priority to a PVC within a Frame Relay map class. |
| frame-relay pvc | Configures Frame Relay PVCs for FRF.8 Frame Relay-ATM Service Interworking. |
| service-policy | Attaches a policy map to an input interface or VC or an output interface or VC. |
| show dial-peer voice | Displays configuration information and call statistics for dial peers. |
| show frame-relay fragment | Displays Frame Relay fragmentation details. |
| show frame-relay map | Displays the current Frame Relay map entries and information about the connections |
| show frame-relay vc-bundle | Displays attributes and other information about a Frame Relay PVC bundle. |

show glbp

To display Gateway Load Balancing Protocol (GLBP) information, use the **show glbp** command in privileged EXEC mode.

```
show glbp [capability [interface-type interface-number ]] | [[interface-type interface-number
[group-number] [state] [brief] [detail] [client-cache [[age number] [forwarder number]]] |
[mac-address address] | [summary]]]
```

Syntax Description

| | |
|--|---|
| <i>interface-type</i> <i>interface-number</i> | (Optional) Interface type and number for which output is displayed. |
| <i>group-number</i> | (Optional) GLBP group number in the range from 0 to 1023. |
| <i>state</i> | (Optional) State of the GLBP router, one of the following: active , disabled , init , listen , and standby . |
| brief | (Optional) Summarizes each virtual gateway or virtual forwarder with a single line of output. |
| detail | (Optional) Displays all the status of the GLBP router in detailed format. The available status are: active , disabled , init , listen , speak , and standby . |
| capability | (Optional) Displays the GLBP capability interfaces. |
| client-cache | (Optional) Displays the GLBP client cache. |
| age number | (Optional) Displays the client-cache age in the range from 0 to 1440. |
| forwarder number | (Optional) Displays the client forwarder in the range from 1 to 4. |
| mac-address <i>address</i> | (Optional) Displays the mac-address of the client. |
| summary | (Optional) Displays the summary of the GLBP client caches. |

Command Modes

Privileged EXEC (#)

Command History

| Release | Modification |
|--------------------------|--|
| 12.2(14)S | This command was introduced. |
| 12.2(15)T | This command was integrated into Cisco IOS Release 12.2(15)T. The client-cache keyword was added. |
| 12.3(2)T | The output was enhanced to display information about Message Digest 5 (MD5) authentication. |
| 12.3(7)T | The output was enhanced to display information about assigned redundancy names to specified groups. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(31)SB2 | This command was enhanced to display information about GLBP support of Stateful Switchover (SSO) mode. |
| 12.2(33)SXH | This command was integrated into Cisco IOS Release 12.2(33)SXH. |
| Cisco IOS XE Release 2.1 | This command was integrated into Cisco IOS XE Release 2.1. |

| Release | Modification |
|--------------|---|
| 12.4(15)T | This command was modified. The client-cache keyword was added. |
| 12.4(24)T | This command was modified. The detail keyword was added. The output was modified to hide configured passwords when MD5 key-string or text authentication is configured. |
| 12.2(33)SXII | This command was modified. The client-cache keyword was added. The output was modified to hide configured passwords when MD5 key-string or text authentication is configured. |
| 12.2(33)SRE | The output was modified to hide configured passwords when MD5 key-string or text authentication is configured. |

Usage Guidelines

Use the **show glbp** command to display information about GLBP groups on a router. The **brief** keyword displays a single line of information about each virtual gateway or virtual forwarder. The **client-cache** keyword displays the client cache details and the **capability** keyword displays all GLBP-capable interfaces.

Examples

The following is sample output from the **show glbp** command:

```
Router# show glbp

FastEthernet0/0 - Group 10
  State is Active
    2 state changes, last state change 23:50:33
  Virtual IP address is 10.21.8.10
  Hello time 5 sec, hold time 18 sec
    Next hello sent in 4.300 secs
  Redirect time 600 sec, forwarder time-out 7200 sec
  Authentication MD5, key-string
  Preemption enabled, min delay 60 sec
  Active is local
  Standby is unknown
  Priority 254 (configured)
  Weighting 105 (configured 110), thresholds: lower 95, upper 105
    Track object 2 state Down decrement 5
  Load balancing: host-dependent
  There is 1 forwarder (1 active)
  Forwarder 1
    State is Active
      1 state change, last state change 23:50:15
    MAC address is 0007.b400.0101 (default)
    Owner ID is 0005.0050.6c08
  Redirection enabled
  Preemption enabled, min delay 60 sec
  Active is local, weighting 105
```

The following is sample output from the **show glbp** command with the **brief** keyword specified:

```
Router# show glbp brief

Interface  Grp  Fwd Pri State   Address           Active router  Standby router
Fa0/0     10   -   254 Active  10.21.8.10       local          unknown
Fa0/0     10   1   7   Active  0007.b400.0101  local          -
```

The following is sample output from the **show glbp** command that displays GLBP group 10:


```

Router# show glbp 10

FastEthernet0/0 - Group 10
  State is Active
    2 state changes, last state change 23:50:33
  Virtual IP address is 10.21.8.10
  Hello time 5 sec, hold time 18 sec
    Next hello sent in 4.300 secs
  Redirect time 600 sec, forwarder time-out 7200 sec
  Authentication MD5, key-string
  Preemption enabled, min delay 60 sec
  Active is local
  Standby is unknown
  Priority 254 (configured)
  Weighting 105 (configured 110), thresholds: lower 95, upper 105
    Track object 2 state Down decrement 5
  Load balancing: host-dependent
  There is 1 forwarder (1 active)
  Forwarder 1
    State is Active
      1 state change, last state change 23:50:15
    MAC address is 0007.b400.0101 (default)
    Owner ID is 0005.0050.6c08
    Redirection enabled
    Preemption enabled, min delay 60 sec
    Active is local, weighting 105

```

The following output shows that the redundancy name has been assigned to the “glbp1” group:

```

Router# show glbp ethernet0/1 1

Ethernet0/1 - Group 1
  State is Listen
    64 state changes, last state change 00:00:54
  Virtual IP address is 10.1.0.7
  Hello time 50 msec, hold time 200 msec
    Next hello sent in 0.030 secs
  Redirect time 600 sec, forwarder time-out 14400 sec
  Authentication text, string "authword"
  Preemption enabled, min delay 0 sec
  Active is 10.1.0.2, priority 105 (expires in 0.184 sec)
  Standby is 10.1.0.3, priority 100 (expires in 0.176 sec)
  Priority 96 (configured)
  Weighting 100 (configured 100), thresholds: lower 95, upper 100
    Track object 1 state Up decrement 10
  Load balancing: round-robin
  IP redundancy name is "glbp1"
  Group members:
    0004.4d83.4801 (10.0.0.0)
    0010.7b5a.fa41 (10.0.0.1)
    00d0.bbd3.bc21 (10.0.0.2) local

```

The following output shows GLBP support for SSO mode on an active RP:

```

Router# show glbp

Ethernet0/0 - Group 1
  State is Standby
    1 state change, last state change 00:00:20
  Virtual IP address is 172.24.1.254
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.232 secs
  Redirect time 600 sec, forwarder time-out 14400 sec
  Preemption disabled

```

```

Active is 172.24.1.2, priority 100 (expires in 7.472 sec)
Standby is local
Priority 100 (default)
Weighting 100 (default 100), thresholds: lower 1, upper 100
Load balancing: round-robin
Group members:
aabb.cc00.0100 (172.24.1.1) local
aabb.cc00.0200 (172.24.1.2)
There are 2 forwarders (1 active)
Forwarder 1
State is Listen
MAC address is 0007.b400.0101 (learnt)
Owner ID is aabb.cc00.0200
Time to live: 14397.472 sec (maximum 14400 sec)
Preemption enabled, min delay 30 sec
Active is 172.24.1.2 (primary), weighting 100 (expires in 9.540 sec)
Forwarder 2
State is Active
1 state change, last state change 00:00:28
MAC address is 0007.b400.0102 (default)
Owner ID is aabb.cc00.0100
Preemption enabled, min delay 30 sec
Active is local, weighting 100

```

The following output shows GLBP support for SSO mode on a standby RP:

```
RouterRP-standby# show glbp
```

```

Ethernet0/0 - Group 1
State is Init (standby RP, peer state is Standby)
Virtual IP address is 172.24.1.254
Hello time 3 sec, hold time 10 sec
Redirect time 600 sec, forwarder time-out 14400 sec
Preemption disabled
Active is unknown
Standby is unknown
Priority 100 (default)
Weighting 100 (default 100), thresholds: lower 1, upper 100
Load balancing: round-robin
Group members:
aabb.cc00.0100 (172.24.1.1) local
aabb.cc00.0200 (172.24.1.2)
There are 2 forwarders (0 active)
Forwarder 1
State is Init (standby RP, peer state is Listen)
MAC address is 0007.b400.0101 (learnt)
Owner ID is aabb.cc00.0200
Preemption enabled, min delay 30 sec
Active is unknown
Forwarder 2
State is Init (standby RP, peer state is Active)
MAC address is 0007.b400.0102 (default)
Owner ID is aabb.cc00.0100
Preemption enabled, min delay 30 sec
Active is unknown

```

GLBP support for Stateful Switchover (SSO) mode is enabled by default but may be disabled by the **no glbp sso** command. If GLBP support for SSO mode is disabled, the output of the **show glbp** command on the standby RP will display a warning:

```
RouterRP-standby# show glbp
```

```

Ethernet0/0 - Group 1
State is Init (GLBP SSO disabled) <----- GLBP SSO is disabled.

```

```

Virtual IP address is 172.24.1.254
Hello time 3 sec, hold time 10 sec
Redirect time 600 sec, forwarder time-out 14400 sec
Preemption disabled
Active is unknown
Standby is unknown
Priority 100 (default)
Weighting 100 (default 100), thresholds: lower 1, upper 100
Load balancing: round-robin
Group members:
aabb.cc00.0100 (172.24.1.1) local
There are 2 forwarders (0 active)
Forwarder 1
State is Init (GLBP SSO disabled)
MAC address is 0007.b400.0101 (learnt)
Owner ID is aabb.cc00.0200
Preemption enabled, min delay 30 sec
Active is unknown
Forwarder 2
State is Init (GLBP SSO disabled)
MAC address is 0007.b400.0102 (default)
Owner ID is aabb.cc00.0100
Preemption enabled, min delay 30 sec
Active is unknown

```

Table 84 describes the significant fields shown in the displays.

Table 84 *show glbp Field Descriptions*

| Field | Description |
|-------------------------|--|
| FastEthernet0/0 - Group | Interface type and number and GLBP group number for the interface. |
| State is | <p>State of the virtual gateway or virtual forwarder. For a virtual gateway, the state can be one of the following:</p> <ul style="list-style-type: none"> • Active—The gateway is the active virtual gateway (AVG) and is responsible for responding to Address Resolution Protocol (ARP) requests for the virtual IP address. • Disabled—The virtual IP address has not been configured or learned yet, but another GLBP configuration exists. • Initial—The virtual IP address has been configured or learned, but virtual gateway configuration is not complete. An interface must be up and configured to route IP, and an interface IP address must be configured. • Listen—The virtual gateway is receiving hello packets and is ready to change to the “speak” state if the active or standby virtual gateway becomes unavailable. • Speak—The virtual gateway is attempting to become the active or standby virtual gateway. • Standby—The gateway is next in line to be the AVG. |

Table 84 *show glbp Field Descriptions (continued)*

| Field | Description |
|-----------------------|--|
| | <p>For a virtual forwarder, the state can be one of the following:</p> <ul style="list-style-type: none"> • Active—The gateway is the active virtual forwarder (AVF) and is responsible for forwarding packets sent to the virtual forwarder MAC address. • Disabled—The virtual MAC address has not been assigned or learned. This is a transitory state because a virtual forwarder changing to a disabled state is deleted. • Initial—The virtual MAC address is known, but virtual forwarder configuration is not complete. An interface must be up and configured to route IP, an interface IP address must be configured, and the virtual IP address must be known. • Listen—The virtual forwarder is receiving hello packets and is ready to change to the “active” state if the AVF becomes unavailable. |
| Virtual IP address is | The virtual IP address of the GLBP group. All secondary virtual IP addresses are listed on separate lines. If one of the virtual IP addresses is a duplicate of an address configured for another device, it will be marked as “duplicate.” A duplicate address indicates that the router has failed to defend its ARP cache entry. |
| Hello time, hold time | The hello time is the time between hello packets (in seconds or milliseconds). The hold time is the time (in seconds or milliseconds) before other routers declare the active router to be down. All routers in a GLBP group use the hello- and hold-time values of the current AVG. If the locally configured values are different, the configured values appear in parentheses after the hello- and hold-time values. |
| Next hello sent in | The time until GLBP will send the next hello packet (in seconds or milliseconds). |
| Preemption | <p>Whether GLBP gateway preemption is enabled. If enabled, the minimum delay is the time (in seconds) for which a higher-priority nonactive router will wait before preempting the lower-priority active router.</p> <p>This field is also displayed under the forwarder section where it indicates GLBP forwarder preemption.</p> |
| Active is | <p>The active state of the virtual gateway. The value can be “local,” “unknown,” or an IP address. The address (and the expiration date of the address) is the address of the current AVG.</p> <p>This field is also displayed under the forwarder section where it indicates the address of the current AVF.</p> |
| Standby is | The standby state of the virtual gateway. The value can be “local,” “unknown,” or an IP address. The address (and the expiration date of the address) is the address of the standby gateway (the gateway that is next in line to be the AVG). |
| Weighting | The initial weighting value with lower and upper threshold values. |
| Track object | The list of objects that are being tracked and their corresponding states. |
| IP redundancy name is | The name of the GLBP group. |

Related Commands

| Command | Description |
|-----------------------------|---|
| glbp ip | Enables GLBP. |
| glbp timers | Configures the time between hello messages and the time before other routers declare the active GLBP router to be down. |
| glbp weighting track | Specifies an object to be tracked that affects the weighting of a GLBP gateway. |

show interfaces accounting

To display the number of packets of each protocol type that have been sent through all configured interfaces, use the **show interfaces accounting** command in user EXEC or privileged EXEC mode.

show interfaces [*interface type number* | **null** *interface-number* | **vlan** *vlan-id*] **accounting**

Syntax Description

| | |
|--|---|
| <i>interface</i> | (Optional) Interface type; possible valid values are ethernet , fastethernet , gigabitethernet , tengigabitethernet , pos , and port-channel , atm , and ge-wan . |
| <i>type number</i> | (Optional) Module and port number; see the “Usage Guidelines” section for valid values. |
| null <i>interface-number</i> | (Optional) Specifies the null interface; the valid value is 0 . |
| vlan <i>vlan-id</i> | (Optional) Specifies the VLAN ID; valid values are from 1 to 4094. |

Command Modes

User EXEC
Privileged EXEC

Command History

| Release | Modification |
|--------------------------|---|
| 12.2(17a)SX1 | This command was introduced on the Supervisor Engine 720. |
| 12.2(17d)SXB | Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(33)SRC | Support for IPv6 was added. |
| 12.2(33)SB | This command was integrated into Cisco IOS Release 12.2(33)SB. |
| Cisco IOS XE Release 2.1 | This command was introduced on Cisco ASR 1000 Series Routers. |

Usage Guidelines



Note

The Pkts Out and Chars Out fields display IPv6 packet counts only. The Pkts In and Chars In fields display both IPv4 and IPv6 packet counts, except for tunnel interfaces. For tunnel interfaces, the IPv6 input packets are counted as IPv6 packets only.

Due to hardware limitations on the ASIC, PFC IPv4 and IPv6 packets cannot be differentiated in the Pkts In and Chars In fields for IP count the IPv6 and IPv4 packets that are hardware forwarded. The Pkts In and Chars In fields for IPv6 only count software-forwarded packets. The IP Pkts Out and Chars Out fields show IPv4 packets, and the IPv6 Pkts Out and Chars Out fields show IPv6 packets.

The *interface-number* argument designates the module and port number. Valid values for *interface-number* depend on the specified interface type and the chassis and module that are used. For example, if you specify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the module number are from 1 to 13 and valid values for the port number are from 1 to 48.

The port channels from 257 to 282 are internally allocated and are supported on the CSM and the FWSM only.

If you do not enter any keywords, all counters for all modules are displayed.

Examples

This example shows how to display the number of packets of each protocol type that have been sent through all configured interfaces:

```
Router> show interfaces gigabitethernet 5/2 accounting
```

```
GigabitEthernet5/2
Protocol Pkts In Chars In Pkts Out Chars Out
IP       50521  50521000 0      0
DEC MOP  0      0        1      129
CDP     0      0        1      592
IPv6    11     834     96     131658
Router#
```

Table 85 describes the significant fields shown in the display.

Table 85 show interfaces accounting Command Output Fields

| Field | Description |
|-----------|---|
| Protocol | Protocol that is operating on the interface. |
| Pkts In | For IP it is the number of IPv4 software switched, IPv4 and IPv6 hardware switched packets received for the specified protocol. For IPv6 it is the number of IPv6 software switched packets received for the specified protocol. |
| Chars In | For IP it is the number of IPv4 software switched, IPv4 and IPv6 hardware switched characters received for the specified protocol. For IPv6 it is the number of IPv6 software switched characters received for the specified protocol. |
| Pkts Out | For IP it is the number of IPv4 software and hardware switched packets transmitted for the specified protocol. For IPv6 it is the number of IPv6 software and hardware switched packets transmitted for the specified protocol. |
| Chars Out | For IP it is the number of IPv4 software and hardware switched characters transmitted for the specified protocol. For IPv6 it is the number of IPv6 software and hardware switched characters transmitted for the specified protocol. |

Related Commands

| Command | Description |
|-----------------|---|
| show interfaces | Displays the status and statistics for the interfaces in the chassis. |

show ip sockets

To display IP socket information, use the **show ip sockets** command in user EXEC or privileged EXEC mode.

show ip sockets

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

| Release | Modification |
|-------------|--|
| 10.0 T | This command was introduced. |
| 12.2(2)T | Support for IPv6 socket information in the display output of the command was added. |
| 12.0(21)ST | This command was integrated into Cisco IOS Release 12.0(21)ST. |
| 12.0(22)S | This command was integrated into Cisco IOS Release 12.0(22)S. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |
| 12.2(28)SB | This command was integrated into Cisco IOS Release 12.2(28)SB. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.4(11)T | This command was replaced by the show udp , show sockets and show ip sctp commands. |
| 12.2(33)SXH | This command was integrated into Cisco IOS Release 12.2(33)SXH. |

Usage Guidelines

Use this command to verify that the socket being used is opening correctly. If there is a local and remote endpoint, a connection is established with the ports indicated.

Examples

The following is sample output from the **show ip sockets** command:

```
Router# show ip sockets
```

| Proto | Remote | Port | Local | Port | In | Out | Stat | TTY | OutputIF |
|-------|----------------|-------|----------------|------|----|-----|------|-----|----------|
| 17 | 10.0.0.0 | 0 | 172.16.186.193 | 67 | 0 | 0 | 1 | 0 | |
| 17 | 172.16.191.135 | 514 | 172.16.191.129 | 1811 | 0 | 0 | 0 | 0 | |
| 17 | 172.16.135.20 | 514 | 172.16.191.1 | 4125 | 0 | 0 | 0 | 0 | |
| 17 | 172.16.207.163 | 49 | 172.16.186.193 | 49 | 0 | 0 | 9 | 0 | |
| 17 | 10.0.0.0 | 123 | 172.16.186.193 | 123 | 0 | 0 | 1 | 0 | |
| 88 | 10.0.0.0 | 0 | 172.16.186.193 | 202 | 0 | 0 | 0 | 0 | |
| 17 | 172.16.96.59 | 32856 | 172.16.191.1 | 161 | 0 | 0 | 1 | 0 | |
| 17 | --listen-- | | --any-- | 496 | 0 | 0 | 1 | 0 | |

The following sample output from the **show ip sockets** command shows IPv6 socket information:

```
Router# show ip sockets
```

```

Proto   Remote   Port    Local   Port    In     Out    Stat    TTY  OutputIF
17(v6)  --listen-- --any-- 1024    0       0      0       0
17(v6)  --listen-- --any-- 7       0       0      0       0
17(v6)  --listen-- --any-- 161    0       0      0       0
17(v6)  --listen-- --any-- 162    0       0      0       0
17      --listen-- --any-- 1024    0       0      0       0
17      --listen-- --any-- 7       0       0      0       0
17      --listen-- --any-- 9       0       0      0       0
17      --listen-- --any-- 19      0       0      0       0
17      --listen-- --any-- 1645   0       0      0       0
17      --listen-- --any-- 1646   0       0      0       0
17      --listen-- --any-- 161    0       0      0       0
17      --listen-- --any-- 162    0       0      0       0

```

Table 86 describes the significant fields shown in the display.

Table 86 show ip sockets Field Descriptions

| Field | Description |
|----------|---|
| Proto | Protocol type, for example, User Datagram Protocol (UDP) or TCP. |
| Remote | Remote address connected to this networking device. If the remote address is considered illegal, "--listen--" is displayed. |
| Port | Remote port. If the remote address is considered illegal, "--listen--" is displayed. |
| Local | Local address. If the local address is considered illegal or is the address 0.0.0.0, "--any--" displays. |
| Port | Local port. |
| In | Input queue size. |
| Out | Output queue size. |
| Stat | Various statistics for a socket. |
| TTY | The tty number for the creator of this socket. |
| OutputIF | Output IF string, if one exists. |
| v6 | IPv6 sockets. |

Related Commands

| Command | Description |
|----------------|---|
| show ip sctp | Displays information about SCTP. |
| show processes | Displays information about the active processes. |
| show sockets | Displays IP socket information. |
| show udp | Displays IP socket information about UDP processes. |

show ipv6 access-list

To display the contents of all current IPv6 access lists, use the **show ipv6 access-list** command in user EXEC or privileged EXEC mode.

```
show ipv6 access-list [access-list-name]
```

| | |
|---------------------------|---|
| Syntax Description | <i>access-list-name</i> (Optional) Name of access list. |
|---------------------------|---|

Command Default All IPv6 access lists are displayed.

Command Modes User EXEC
Privileged EXEC

| Command History | Release | Modification |
|-----------------|-------------|--|
| | 12.2(2)T | This command was introduced. |
| | 12.0(21)ST | This command was integrated into Cisco IOS Release 12.0(21)ST. |
| | 12.0(22)S | This command was integrated into Cisco IOS Release 12.0(22)S. |
| | 12.0(23)S | The priority field was changed to sequence and Layer 4 protocol information (extended IPv6 access list functionality) was added to the display output. |
| | 12.2(13)T | This command was integrated into 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(28)SB | This command was integrated into Cisco IOS Release 12.2(28)SB. |
| | 12.2(25)SG | This command was integrated into Cisco IOS Release 12.2(25)SG. |
| | 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. |
| | 12.2(50)SY | This command was modified. Information about IPv4 and IPv6 hardware statistics is displayed. |

Usage Guidelines The **show ipv6 access-list** command provides output similar to the **show ip access-list** command, except that it is IPv6-specific.

Examples The following output from the **show ipv6 access-list** command shows IPv6 access lists named inbound, tcptraffic, and outbound:

```
Router# show ipv6 access-list
```

```
IPv6 access list inbound
  permit tcp any any eq bgp reflect tcptraffic (8 matches) sequence 10
  permit tcp any any eq telnet reflect tcptraffic (15 matches) sequence 20
  permit udp any any reflect udptraffic sequence 30
```

show ipv6 access-list

```
IPv6 access list tcptraffic (reflexive) (per-user)
  permit tcp host 2001:0DB8:1::1 eq bgp host 2001:0DB8:1::2 eq 11000 timeout 300 (time
    left 243) sequence 1
  permit tcp host 2001:0DB8:1::1 eq telnet host 2001:0DB8:1::2 eq 11001 timeout 300
    (time left 296) sequence 2
```

```
IPv6 access list outbound
  evaluate udptraffic
  evaluate tcptraffic
```

The following sample output shows IPv6 access list information for use with IPsec:

```
Router# show ipv6 access-list
IPv6 access list Tunnel0-head-0-ACL (crypto)
  permit ipv6 any any (34 matches) sequence 1
IPv6 access list Ethernet2/0-ipsecv6-ACL (crypto)
  permit 89 FE80::/10 any (85 matches) sequence 1
```

Table 87 describes the significant fields shown in the display.

Table 87 *show ipv6 access-list Field Descriptions*

| Field | Description |
|--------------------------|---|
| ipv6 access list inbound | Name of the IPv6 access list, for example, inbound. |
| permit | Permits any packet that matches the specified protocol type. |
| tcp | Transmission Control Protocol. The higher-level (Layer 4) protocol type that the packet must match. |
| any | Equal to ::/0. |
| eq | An equal operand that compares the source or destination ports of TCP or UDP packets. |
| bgp | Border Gateway Protocol. The lower-level (Layer 3) protocol type that the packet must be equal to. |
| reflect | Indicates a reflexive IPv6 access list. |
| tcptraffic (8 matches) | The name of the reflexive IPv6 access list and the number of matches for the access list. The clear ipv6 access-list privileged EXEC command resets the IPv6 access list match counters. |
| sequence 10 | Sequence in which an incoming packet is compared to lines in an access list. Lines in an access list are ordered from first priority (lowest number, for example, 10) to last priority (highest number, for example, 80). |
| host 2001:0DB8:1::1 | The source IPv6 host address that the source address of the packet must match. |
| host 2001:0DB8:1::2 | The destination IPv6 host address that the destination address of the packet must match. |
| 11000 | The ephemeral source port number for the outgoing connection. |
| timeout 300 | The total interval of idle time (in seconds) after which the temporary IPv6 reflexive access list named tcptraffic will time out for the indicated session. |

Table 87 *show ipv6 access-list Field Descriptions (continued)*

| Field | Description |
|---------------------|--|
| (time left 243) | The amount of idle time (in seconds) remaining before the temporary IPv6 reflexive access list named tcptraffic is deleted for the indicated session. Additional received traffic that matches the indicated session resets this value to 300 seconds. |
| evaluate udptraffic | Indicates the IPv6 reflexive access list named udptraffic is nested in the IPv6 access list named outbound. |

Related Commands

| Command | Description |
|-------------------------------|---|
| clear ipv6 access-list | Resets the IPv6 access list match counters. |
| hardware statistics | Enables the collection of hardware statistics. |
| show ip access-list | Displays the contents of all current IP access lists. |
| show ip prefix-list | Displays information about a prefix list or prefix list entries. |
| show ipv6 prefix-list | Displays information about an IPv6 prefix list or IPv6 prefix list entries. |

show ipv6 cef

To display entries in the IPv6 Forwarding Information Base (FIB), use the **show ipv6 cef** command in user EXEC or privileged EXEC mode.

Privileged EXEC Mode

```
show ipv6 cef [interface-type number [platform] [checksum | detail | internal [checksum]] |
  ipv6-prefix[/prefix-length] [dependents | longer-prefixes [platform] [checksum | detail |
  internal [checksum]] | similar-prefixes | platform [checksum | detail | internal [checksum]]
  | epoch | prefix-statistics | checksum | detail | internal [checksum]]
```

User EXEC Mode

```
show ipv6 cef [ipv6-prefix[/prefix-length] [dependents | detail | longer-prefixes [platform]
  [detail] | similar-prefixes] | interface-type interface-number [platform] [detail] | epoch |
  prefix-statistics]
```

| Syntax Description | Description |
|-------------------------|--|
| <i>ipv6-prefix</i> | (Optional) IPv6 network assigned to the interface. <ul style="list-style-type: none"> This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons. |
| <i>/prefix-length</i> | (Optional) The IPv6 network assigned to the interface and the length of the IPv6 prefix. <ul style="list-style-type: none"> The <i>ipv6-prefix</i> must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons. The <i>prefix-length</i> is a decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value. |
| longer-prefixes | (Optional) Displays FIB information for more specific destinations. |
| <i>interface-type</i> | (Optional) Interface type. For more information, use the question mark (?) online help function. |
| <i>interface-number</i> | (Optional) Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function. |
| platform | (Optional) Displays platform-specific Cisco Express Forwarding data. |
| detail | (Optional) Displays detailed FIB entry information. |
| internal | (Optional) Displays internal FIB entry information. |
| checksum | (Optional) Displays FIB entry checksums. |
| dependents | (Optional) Displays dependents of the selected prefix. |
| similar-prefixes | (Optional) Displays FIB information for prefixes that are similar to one another. |
| epoch | (Optional) Displays the basic FIB entries filtered by epoch number. |
| summary | (Optional) Displays the summary of events log. |

| | |
|------------------------------|--|
| new | (Optional) Displays new events since the last show operation was performed. |
| within <i>minutes</i> | (Optional) Displays events within the specified time, in minutes. The range is from 1 to 4294967295. |
| prefix-statistics | (Optional) Displays nonzero prefix statistics. |

Command Default

If no keyword or argument is specified, information about all FIB entries is displayed.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

| Release | Modification |
|--------------------------|--|
| 12.0(21)ST | This command was introduced. |
| 12.0(22)S | This command was modified. The <i>interface-type</i> and <i>interface-number</i> arguments and the longer-prefixes and detail keywords were added. |
| 12.2(13)T | This command was integrated into 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(25)S | This command was modified. The dependents , events , internal , new , platform , similar-prefixes and within keywords were added. |
| 12.2(28)SB | This command was integrated into Cisco IOS Release 12.2(28)SB. |
| 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. |
| Cisco IOS XE Release 2.1 | This command was introduced on Cisco ASR 1000 Series Routers. |

Usage Guidelines

The **show ipv6 cef** command is similar to the **show ip cef** command, except that it is IPv6-specific.

Examples

The following is sample output from the **show ipv6 cef** command when no keywords or arguments are entered:

```
Router# show ipv6 cef

Global IPv6 CEF Table
12 prefixes

2FFE::3/128
  Receive
2FFE::/64
  attached to POS3/1
3FFE::/64
  nexthop FE80::yyyy:4AFF:FE6D:B980 POS3/1
  nexthop FE80::xxxx:7DFE:FE8D:A840 FastEthernet1/0
3FFE:zz::3/128
  Receive
3FFE:zz::/64
```

```

    attached to FastEthernet1/0
3FFE:rr::3/128
    Receive
3FFE:rr::/64
    attached to FastEthernet1/1
3FFE:pp::3/128
    Receive
3FFE:pp::/64
    attached to FastEthernet1/2
3FFE:mnnn:2222::/64
    nexthop::POS3/1
3FFE:ssss::/64
    recursive via 2FFE::2 POS3/1
FE80::/64
    Receive

```

The following is sample output from the **show ipv6 cef** command showing 6PE multipath information:

```

Router# show ipv6 cef

Global IPv6 CEF Table
12 prefixes
.
.
.
nexthop 10.1.1.3 Ethernet0/0 label 25 16
4004::/64
    nexthop 10.1.1.3 Ethernet0/0 label 27 16
    nexthop 10.1.1.3 Ethernet0/0 label 26 18

```

[Table 88](#) describes the significant fields shown in the displays.

Table 88 *show ipv6 cef Field Descriptions*

| Field | Description |
|---|--|
| 12 prefixes | Indicates the total number of IPv6 prefixes in the Cisco Express Forwarding table. |
| 2FFE::3/128 | Indicates the IPv6 prefix of the remote network. |
| Receive | Indicates that this IPv6 prefix is local to the router. |
| 3FFE::/64 nexthop FE80::yyyy:4AFF:FE6D:B980 POS3/1 nexthop FE80::xxxx:7DFE:FE8D:A840 FastEthernet1/0 | Indicates that IPv6 prefix 3FFE::/64 is reachable through these next hop addresses and interfaces. <ul style="list-style-type: none"> Multiple next-hop entries are shown for IPv6 prefixes that have load sharing. |
| attached to FastEthernet1/0 | Indicates that this IPv6 prefix is a connected network on Fast Ethernet interface 1/0. |
| recursive via 2FFE::2 POS3/1 | Indicates that this IPv6 prefix uses the same forwarding information as 2FFE::2 POS3/1. |

The following is sample output from the **show ipv6 cef detail** command for Fast Ethernet interface 1/0:

```

Router# show ipv6 cef fastethernet 1/0 detail

IPv6 CEF is enabled and running
IPv6 CEF default table
2 prefixes
3FFE:zz::/64

```

```

    attached to FastEthernet1/0
3FFE:rr::/64
    attached to FastEthernet1/1

```

The fields in the are self-explanatory.

The following is sample output from the **show ipv6 cef longer-prefixes** command for the IPv6 prefix 3FFE:xxxx:20:1::12/128. The fields in the display are self-explanatory.

```
Router# show ipv6 cef 3FFE:xxxx:20:1::12/128 longer-prefixes
```

```

IPv6 CEF is enabled and running
IPv6 CEF default table
2 prefixes
3FFE:xxxx:20:1::12/128 Receive
    Receive
3FFE:xxxx:20:1::/64 Attached, Connected
    attached to Tunnel81

```

The following is sample output from the **show ipv6 cef detail** command showing 6PE multipath information. The prefix 4004::/64 is received by the Border Gateway Protocol (BGP) from two different peers and therefore two different paths.

```
Router# show ipv6 cef detail
```

```

IPv6 CEF is enabled and running
VRF Default:
 20 prefixes (20/0 fwd/non-fwd)
  Table id 0, version 20, 0 resets
  Database epoch:0 (20 entries at this epoch)
.
.
.
4004::/64, epoch 0, per-destination sharing
  recursive via 172.11.11.1 label 27
  nexthop 10.1.1.3 Ethernet0/0 label 16
  recursive via 172.30.30.1 label 26
  nexthop 10.1.1.3 Ethernet0/0 label 18

```

The fields in the display are self-explanatory.

The following is sample output from the **show ipv6 cef internal** command:

```
Router# show ipv6 cef internal
```

```

IPv6 CEF is enabled and running
Slow processing intvl = 1 seconds backoff level current/max 0/0
0 unresolved prefixes, 0 requiring adjacency update
IPv6 CEF default table
14 prefixes tableid 0
table version 17
root 6283F5D0
.
.
.
BEEF:20::/64 RIBfib <=====entry with two mpls path
Using loadinfo 0x62A75194
  loadinfo ptr 62A75194 flags 0000 next hash = 0
  refcount 3 path list ptr 0x00000000
  hashes :-
    62335678 drop adjacency
.
.
.
  path list pointer 62370FA0

```



```

2 paths -
  Nexthop path_pointer 6236E420 traffic share 1 path_list pointer 62370FA0
  nexthop ::FFFF:172.12.12.1
  next_hop_len 0 adjacency pointer 62335678
  Nexthop path_pointer 6236E480 traffic share 1 path_list pointer 62370FA0
  nexthop ::FFFF:172.14.14.1
  next_hop_len 0 adjacency pointer 62335678
refcount 2
1 loadinfos -
  loadinfo ptr 62A75194 flags 0000 next hash = 0
  refcount 3 path list ptr 0x00000000
  hashes :-
    62335678 drop adjacency
    .
    .
tag information
  local tag: exp-null
  rewrites :-
    Fa0/1, 10.2.1.1, tags imposed: {32}
    Fa1/0, 10.1.1.3, tags imposed: {25}
    Fa0/1, 10.2.1.1, tags imposed: {32}
    Fa1/0, 10.1.1.3, tags imposed: {25}
    Fa0/1, 10.2.1.1, tags imposed: {32}
    Fa1/0, 10.1.1.3, tags imposed: {25}
    Fa0/1, 10.2.1.1, tags imposed: {32}
    Fa1/0, 10.1.1.3, tags imposed: {25}
    Fa0/1, 10.2.1.1, tags imposed: {32}
    Fa1/0, 10.1.1.3, tags imposed: {25}
    Fa0/1, 10.2.1.1, tags imposed: {32}
    Fa1/0, 10.1.1.3, tags imposed: {25}
    Fa0/1, 10.2.1.1, tags imposed: {32}
    Fa1/0, 10.1.1.3, tags imposed: {25}
FE80::/10 Receive, RIBfib
  Receive
FF00::/8 Receive, RIBfib
  Receive

```

Table 88 and Table 89 describe the significant fields shown in displays.

Table 89 *show ipv6 cef internal Field Descriptions*

| Field | Description |
|----------------------------|--|
| Slow processing intvl | Displays the slow processing interval, in seconds. |
| backoff level current/max | Displays the backoff level in the ratio current to the maximum backoff value. |
| unresolved prefixes | Displays the total number of unresolved prefixes. |
| requiring adjacency update | Indicates the number of prefixes that have been resolved but the associated forwarding information has not yet been updated to reflect the route resolution. |
| prefixes | Total number of prefixes in the IPv6 Cisco Express Forwarding default table. |
| tableid | ID of the IPv6 Cisco Express Forwarding default table. |
| table version | Version of the IPv6 Cisco Express Forwarding default table. |

Table 89 *show ipv6 cef internal Field Descriptions (continued)*

| Field | Description |
|--------------------------|---|
| root | Root number of the IPv6 Cisco Express Forwarding default table. |
| Using loadinfo | Current load information |
| loadinfo ptr | Load information pointer. |
| flags | Total number of flags. |
| next hash | Next hash value. |
| refcount 3 path list ptr | Location of the refcount 3 path list pointer. |
| hashes | Total number of hashes. |
| Nexthop_path_pointer | Location of the next hop path pointer. |
| path_list pointer | Location of the path list pointer. |
| refcount | Location of the reference counter. |
| loadinfo ptr | Location of the load information pointer. |

The following is sample output from the **show ipv6 cef internal** command showing 6PE multipath information. The fields in the display are self-explanatory.

```
Router# show ipv6 cef internal

4004::/64, version 15, epoch 0, RIB, refcount 3, per-destination sharing
sources:RIB
feature space:
  IPRM:0x00028000
path 01A53DA0, path list 01A4F2E0, share 0, flags recursive, resolved
ifnums:(none)
  path_list contains no resolved destination(s). HW IPv4 notified.
recursive via 172.11.11.1 label 27, fib 01A6CCA0, 1 terminal fib
  path 01A540B0, path list 01A4F5F0, share 1, flags nexthop
  ifnums:(none)
  path_list contains no resolved destination(s). HW IPv4 notified.
  nexthop 10.1.1.3 Ethernet0/0 label 16, mask /0, adjacency IP adj out of
Ethernet0/0, addr 10.1.1.3 01DE9FB0
path 01A53D30, path list 01A4F2E0, share 0, flags recursive, resolved
ifnums:(none)
  path_list contains no resolved destination(s). HW IPv4 notified.
recursive via 172.30.30.1 label 26, fib 01A6CBD0, 1 terminal fib
  path 01A540B0, path list 01A4F5F0, share 1, flags nexthop
  ifnums:(none)
  path_list contains no resolved destination(s). HW IPv4 notified.
  nexthop 10.1.1.3 Ethernet0/0 label 18, mask /0, adjacency IP adj out of
Ethernet0/0, addr 10.1.1.4 01DE9FB0
output chain:
  loadinfo 01A47520, per-session, flags 0011, 2 locks
  flags:Per-session, for-mps-not-at-eos
  16 hash buckets
    <0 > label 27 label 16 TAG adj out of Ethernet0/0, addr 10.1.1.3
01DE9E30
    <1 > label 26 label 18 TAG adj out of Ethernet0/0, addr 10.1.1.3
01DE9E30
    <2 > label 27 label 16 TAG adj out of Ethernet0/0, addr 10.1.1.3
01DE9E30
    <3 > label 26 label 18 TAG adj out of Ethernet0/0, addr 10.1.1.3
01DE9E30
```

```

<4 > label 27 label 16 TAG adj out of Ethernet0/0, addr 10.1.1.3
.
.
.
<15 > label 26 label 18 TAG adj out of Ethernet0/0, addr 10.1.1.3
01DE9E30

```

The following is sample output from the **show ipv6 cef** command, showing information about the Multiprotocol Label Switching (MPLS) labels associated with the FIB table entries for an IPv6 prefix that is configured to be a Cisco 6PE router using MPLS to transport IPv6 traffic over an IPv4 network.

To display label information from the Cisco Express Forwarding table, enter the **show ipv6 cef** command with an IPv6 prefix. The fields in the display are self-explanatory.

```

Router# show ipv6 cef 2001:0DB8::/32

2001:0DB8::/32
  nexthop ::FFFF:192.168.99.70
  fast tag rewrite with Se0/0, point2point, tags imposed {19 20}
fast tag rewrite with Se0/0, point2point, tags imposed {19 20}

```

Sample Output for Cisco IOS Releases 12.2(25)S, 12.2(28)SB, 12.2(33)SRA, 12.2(33)SXH, 12.4(20)T, and Later Releases

The sample output in the following commands was reformatted with the implementation of Cisco Express Forwarding enhancements. The information in the output is the same as it was before the enhancements.

The following is sample output from the **show ipv6 cef internal** command:

```

Router# show ipv6 cef internal

IPv6 CEF is enabled and running
VRF Default:
  20 prefixes (20/0 fwd/non-fwd)
  Table id 0, 0 resets
  Database epoch: 0 (20 entries at this epoch)

2001:1:12::/64, epoch 0, RIB, refcount 3
  sources: RIB
  feature space:
    MFI: path extension list empty
    IPRM: 0x00038000
    IPV6 adj out of POS1/0 635BAFE0
  path 633A9A18, path list 633A732C, share 1, type attached nexthop
  ifnums: (none)
  path_list contains at least one resolved destination(s). HW IPv6 notified.
  nexthop FE80::205:DCFF:FE26:4800 POS1/0, adjacency IPV6 adj out of POS1/0 635BAFE0
  output chain: IPV6 adj out of POS1/0 635BAFE0

```

The fields in the display are self-explanatory.

The following is sample output from the **show ipv6 cef ipv6-prefix/prefix-length internal** command:

```

Router# show ipv6 cef 2001:2:25::/64 internal

2001:2:25::/64 RIBfib
Using cached adjacency 0x629E1CE0
  path list pointer 62A2C310
    1 path -
      Nexthop path_pointer 62A297B0 traffic share 1 path_list pointer 62A2C310
      nexthop FE80::2D0:1FF:FEE4:6800 FastEthernet0/1
      next_hop_len 0 adjacency pointer 629E1CE0
    refcount 10
    no loadinfo

```

The following is sample output from the **show ipv6 cef detail** command. The fields in the display are self-explanatory.

```
Router# show ipv6 cef detail

IPv6 CEF is enabled and running
VRF Default:
  20 prefixes (20/0 fwd/non-fwd)
  Table id 0, 0 resets
  Database epoch: 0 (20 entries at this epoch)

2001:1:12::/64, epoch 0
  nexthop FE80::205:DCFF:FE26:4800 POS1/0
2001:2:13::/64, epoch 0, flags attached, connected
  attached to POS1/0
2001:2:13::2/128, epoch 0, flags receive
```

The following is sample output from the **show ipv6 cef epoch** command. The fields in the display are self-explanatory.

```
Router# show ipv6 cef epoch

Table: Default
  Database epoch: 1 (2 entries at this epoch)
```

Related Commands

| Command | Description |
|--------------------------------|---|
| show cef interface | Displays Cisco Express Forwarding-related interface information. |
| show ipv6 cef adjacency | Displays Cisco Express Forwarding for IPv6 recursive and direct prefixes resolved through an adjacency. |
| show ipv6 route | Displays IPv6 router advertisement information received from onlink routers. |

show ipv6 cef adjacency

To display Cisco Express Forwarding for IPv6 and distributed Cisco Express Forwarding v6 recursive and direct prefixes resolved through an adjacency, use the **show ipv6 cef adjacency** command in user EXEC or privileged EXEC mode.

```
show ipv6 cef adjacency interface-type interface-number ipv6-address [detail | internal |
samecable] [platform [detail | internal | samecable]] [source [internal | epoch epoch-number
[internal | samecable | platform [detail | internal | samecable]]]] [epoch epoch-number
[internal | samecable | platform [detail | internal | samecable]]]]
```

To display Cisco Express Forwarding for IPv6 and distributed Cisco Express Forwarding v6 recursive and direct prefixes resolved through special adjacency types representing nonstandard switching paths, use this form of the **show ip cef adjacency** command in user EXEC or privileged EXEC mode.

```
show ipv6 cef adjacency {adj-null | discard | drop | glean | null | punt} [checksum] [detail]
[internal] [samecable] [platform [checksum | detail | internal | samecable]] [source
[internal | epoch epoch-number [internal | samecable | platform [detail | internal
[checksum] | samecable]]]] [epoch epoch-number [internal | samecable | detail | platform
[detail | internal | samecable]]]]
```

Syntax Description

| | |
|----------------------------------|--|
| <i>interface-type</i> | Interface type for which to display Cisco Express Forwarding adjacency information. |
| <i>interface-number</i> | Interface number for which to display adjacency information. |
| <i>ipv6-address</i> | Next-hop IPv6 address. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons. |
| detail | (Optional) Displays detailed information for each CEFv6 adjacency type entry. |
| internal | (Optional) Displays data for adjacency type entries. |
| samecable | (Optional) Displays the connected (up) interface for adjacency type entries. |
| platform | (Optional) Displays platform-specific adjacency information. |
| source | (Optional) Displays source-specific adjacency information. |
| epoch <i>epoch-number</i> | (Optional) Displays adjacency type entries filtered by epoch number. The epoch number range is from 0 to 255. |
| discard | Displays discard adjacency information. Sets up for loopback interfaces. Loopback IPv6 addresses are receive entries in the FIB table. |
| drop | Displays drop adjacency information. Packets forwarded to this adjacency are dropped. |
| glean | Displays glean adjacency information. Represents destinations on a connected interface for which no Address Resolution Protocol (ARP) cache entry exists. |
| null | Displays null adjacency information. Formed for the null 0 interface. Packets forwarded to this adjacency are dropped. |
| punt | Displays punt adjacency information. Represents destinations that cannot be switched in the normal path and that are punted to the next fastest switching vector. |

| | |
|-----------------|--|
| adj-null | Displays null adjacency information. |
| checksum | (Optional) Displays FIB entry checksums. |

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

| Release | Modification |
|-------------|--|
| 12.0(22)S | This command was introduced. |
| 12.2(13)T | This command was integrated into 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(25)S | This command was modified. The internal , samecable , platform , and source keywords were added. |
| 12.2(28)SB | This command was modified. The null keyword was added. |
| 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

The **show ipv6 cef adjacency** command is similar to the **show ip cef adjacency** command, except that it is IPv6 specific.

This command shows all prefixes resolved through a regular next-hop adjacency or through a special adjacency type such as discard, drop, glean, null, and punt. An adjacency is a node that can be reached by one Layer 2 hop.

Examples

The following is sample output from the **show ipv6 cef adjacency** command when the **glean** type is specified:

```
Router# show ipv6 cef adjacency glean

Prefix          Next Hop          Interface
3FFE:xxxx::/24  attached         Ethernet1
2002::/16       3FFE:xxxx::1     Ethernet1
```

The following is sample output from the **show ipv6 cef adjacency drop** command with **detail** specified:

```
Router# show ipv6 cef adjacency fastethernet 0/1 drop detail

IPv6 CEF is enabled and running
IPv6 CEF default table
12 prefixes
```

The following sample output shows the direct IPv6 prefix when next-hop Ethernet interface 1 is specified:

```
Router# show ipv6 cef adjacency ethernet 1 3FFE:xxxx::250:8BFF:FEE8:F800

Prefix          Next Hop          Interface
3FFE:xxxx::250:8BFF:FEE8:F800/128  2002::/16        Ethernet1
```

Table 90 describes the fields shown in the display.

Table 90 *show ipv6 cef adjacency Field Descriptions*

| Field | Description |
|--------------|--------------------------|
| Prefix | Destination IPv6 prefix. |
| Next Hop | Next-hop IPv6 address. |
| Interface | Next-hop interface. |

Related Commands

| Command | Description |
|------------------------------|--|
| show ipv6 cef summary | Displays a summary of the entries in the IPv6 FIB. |

show ipv6 cef neighbor discovery throttling

To display the Cisco Express Forwarding for IPv6 neighbor discovery (ND) throttling list, use the **show ipv6 cef neighbor discovery throttling** command in privileged EXEC mode.

show ipv6 cef neighbor discovery throttling [internal]

| Syntax Description | internal | (Optional) Displays internal data structures. |
|--------------------|----------|---|
|--------------------|----------|---|

| Command Modes | Privileged EXEC (#) |
|---------------|---------------------|
|---------------|---------------------|

| Command History | Release | Modification |
|-----------------|-------------|---|
| | 12.3(2)T | This command was introduced. |
| | 12.2(28)SB | This command was integrated into Cisco IOS Release 12.2(28)SB. |
| | 12.2(33)SXH | This command was integrated into Cisco IOS Release 12.2(33)SXH. |
| | 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |

Examples

The following is sample output from the **show ipv6 cef neighbor discovery throttling** command:

```
Router# show ipv6 cef neighbor discovery throttling

Address                               Holdtime
2001:1111::1                          00:00:02.296
```

[Table 91](#) describes the fields shown in the display.

Table 91 *show ipv6 cef neighbor discovery throttling Field Descriptions*

| Field | Description |
|----------|---|
| Address | The IPv6 address for which the information on ND throttling list is displayed. |
| Holdtime | Length of time (in hours, minutes, and seconds) that the Cisco IOS software will wait to hear from the peer before declaring it down. |

| Related Commands | Command | Description |
|------------------|----------------------------|-------------------------------------|
| | show ipv6 neighbors | Displays IPv6 ND cache information. |

show ipv6 cef non-recursive

To display nonrecursive route entries in the IPv6 Forwarding Information Base (FIB), use the **show ipv6 cef non-recursive** command in user EXEC or privileged EXEC mode.

```
show ipv6 cef non-recursive [detail | internal | samecable] [platform [detail | internal |
samecable]] [source [internal | epoch epoch-number [internal | samecable | platform [detail
| internal | samecable]]]] [epoch epoch-number [internal | samecable | platform [detail |
internal | samecable]]]
```

Syntax Description

| | |
|----------------------------------|---|
| detail | (Optional) Displays detailed nonrecursive route entry information. |
| internal | (Optional) Displays data for nonrecursive route entries. |
| samecable | (Optional) Displays the connected (up) interface for nonrecursive route entries. |
| platform | (Optional) Displays platform-specific nonrecursive route entries. |
| source | (Optional) Displays source-specific nonrecursive route entry information. |
| epoch <i>epoch-number</i> | (Optional) Displays adjacency type entries filtered by epoch number. The epoch number range is from 0 to 255. |

Command Modes

User EXEC
Privileged EXEC

Command History

| Release | Modification |
|-------------|--|
| 12.0(22)S | This command was introduced. |
| 12.2(13)T | This command was integrated into 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(25)S | The internal , samecable , platform , source , and epoch keywords were added, and the <i>epoch-number</i> argument was added. Next hop information was removed from the command output. |
| 12.2(28)SB | This command was integrated into Cisco IOS Release 12.2(28)SB. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.4(20)T | This command was integrated into Cisco IOS Release 12.4(20)T. |

Usage Guidelines

The **show ipv6 cef non-recursive** command is similar to the **show ip cef non-recursive** command, except that it is IPv6-specific.

The **show ipv6 cef non-recursive detail** command shows detailed FIB entry information for all nonrecursive routes.

Examples

The following is sample output from the **show ipv6 cef non-recursive detail** command:

```
Router# show ipv6 cef non-recursive detail

IPv6 CEF is enabled and running
IPv6 CEF default table
8 prefixes
2001:xx::/35
    nexthop FE80::ssss:CFF:FE3D:DCC9 Tunnel155
2001:zzz:500::/40
    nexthop FE80::nnnn:801A Tunnel132
2001:zzz::/35
    nexthop 3FFE:mmm:8023:21::2 Tunnel126
3FFE:yyy:8023:37::1/128 Receive
    Receive
3FFE:yyy:8023:37::/64 Attached, Connected
    attached to Tunnel137
3FFE:yyy:8023:38::1/128 Receive
    Receive
3FFE:yyy:8023:38::/64 Attached, Connected
    attached to Tunnel140
3FFE:yyy:8023:39::1/128 Receive
    Receive
```

[Table 92](#) describes the significant fields shown in the display.

Table 92 *show ipv6 cef non-recursive Field Descriptions*

| Field | Description |
|---|--|
| 8 prefixes | Indicates the total number of IPv6 prefixes in the Cisco Express Forwarding table. |
| 2001:xx::/35 | Indicates the IPv6 prefix of the remote network. |
| 2001:zzz:500::/40 nexthop FE80::nnnn:801A Tunnel132 | Indicates that IPv6 prefix 2001:zzz:500::/40 is reachable through this next-hop address and interface. |
| attached to Tunnel137 | Indicates that this IPv6 prefix is a connected network on Tunnel interface 37. |
| Receive | Indicates that this IPv6 prefix is local to the router. |

This is an example of the **show ipv6 cef non-recursive** command output in Cisco IOS Releases 12.2(25)S, 12.2(28)SB, 12.2(33)SRA, 12.2(33)SXH, 12.4(20)T, and later releases:

```
Router# show ipv6 cef non-recursive

2003:1::/64
    attached to POS6/1/0
2003:1::1/128
    receive
2003:2::/64
    attached to Loopback0
2003:2::1/128
```

Related Commands

| Command | Description |
|---------------------------------|---|
| show ipv6 cef | Displays entries in the IPv6 FIB. |
| show ipv6 cef summary | Displays a summary of the entries in the IPv6 forwarding FIB. |
| show ipv6 cef unresolved | Displays unresolved entries in the IPv6 FIB. |

show ipv6 cef platform

To display platform-specific Cisco Express Forwarding data, use the **show ipv6 cef platform** command in user EXEC or privileged EXEC mode.

show ipv6 cef platform [**detail** | **internal** | **samecable**]

| Syntax Description | detail | (Optional) Displays detailed platform-specific Cisco Express Forwarding data. |
|--------------------|------------------|---|
| | internal | (Optional) Displays internal platform-specific Cisco Express Forwarding data. |
| | samecable | (Optional) Displays platform-specific data for the connected (up) interface. |

| Command Modes | User EXEC Privileged EXEC |
|---------------|------------------------------|
|---------------|------------------------------|

| Command History | Release | Modification |
|-----------------|-------------|---|
| | 12.2(22)S | This command was introduced. |
| | 12.2(28)SB | This command was integrated into Cisco IOS Release 12.2(28)SB. |
| | 12.2(33)SXH | This command was integrated into Cisco IOS Release 12.2(33)SXH. |
| | 12.2(33)SCE | This command was integrated into Cisco IOS Release 12.2(33)SCE. |

Usage Guidelines If none of the optional keywords is used, data for all platforms is displayed.

Examples The following example will display all platform-specific Cisco Express Forwarding data:

```
Router# show ipv6 cef platform
```

show ipv6 cef summary

To display a summary of the entries in the IPv6 Forwarding Information Base (FIB), use the **show ipv6 cef summary** command in user EXEC or privileged EXEC mode.

```
show ipv6 cef summary
```

Syntax Description This command has no arguments or keywords.

Command Modes User EXEC
Privileged EXEC

| Command History | Release | Modification |
|-----------------|-------------|---|
| | 12.0(22)S | This command was introduced. |
| | 12.2(13)T | This command was integrated into 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(28)SB | This command was integrated into Cisco IOS Release 12.2(28)SB. |
| | 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(20)T | This command was integrated into Cisco IOS Release 12.4(20)T. |

Usage Guidelines The **show ipv6 cef summary** command is similar to the **show ip cef summary** command, except that it is IPv6-specific.

Examples The following is sample output from the **show ipv6 cef summary** command:

```
Router# show ipv6 cef summary

IPv6 CEF is enabled and running
Slow processing intvl = 1 seconds backoff level current/max 0/0
0 unresolved prefixes, 0 requiring adjacency update
IPv6 CEF default table
9 prefixes
```

[Table 93](#) describes the significant fields shown in the display.

Table 93 *show ipv6 cef summary* Field Descriptions

| Field | Description |
|-----------------------|--|
| Slow processing intvl | Indicates the waiting time (in seconds) before the software attempts to resolve any unresolved routes. |

Table 93 *show ipv6 cef summary Field Descriptions (continued)*

| Field | Description |
|----------------------------|--|
| unresolved prefixes | Indicates the number of unresolved routes. |
| requiring adjacency update | Indicates the number of prefixes that have been resolved but the associated forwarding information has not yet been updated to reflect the route resolution. |

This is an example of the **show ipv6 cef summary** command output in Cisco IOS Releases 12.2(25)S, 12.2(28)SB, 12.2(33)SRA, 12.2(33)SXH, 12.4(20)T, and later releases:

```
Router# show ipv6 cef summary

IPv6 CEF is enabled and running
VRF Default:
 20 prefixes (20/0 fwd/non-fwd)
Table id 0, 0 resets
Database epoch: 0 (20 entries at this epoch)
```

Related Commands

| Command | Description |
|---------------------------|--|
| show ipv6 cef | Displays entries in the IPv6 FIB. |
| show cef interface | Displays Cisco Express Forwarding-related interface information. |

show ipv6 cef switching statistics

To display switching statistics in the IPv6 Forwarding Information Base (FIB), use the **show ipv6 cef switching statistics** command in privileged EXEC mode.

show ipv6 cef switching statistics [feature]

| | |
|---------------------------|---|
| Syntax Description | feature (Optional) The output is ordered by feature. |
|---------------------------|---|

| | |
|----------------------|-----------------|
| Command Modes | Privileged EXEC |
|----------------------|-----------------|

| Command History | Release | Modification |
|------------------------|----------------|---|
| | 12.2(25)S | This command was introduced. |
| | 12.2(28)SB | This command was integrated into Cisco IOS Release 12.2(28)SB. |
| | 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(20)T | This command was integrated into Cisco IOS Release 12.4(20)T. |

| | |
|-------------------------|--|
| Usage Guidelines | If the optional feature keyword is not used, all switching statistics are displayed. |
|-------------------------|--|

Examples The following is sample output from the **show ipv6 cef switching statistics** command:

```
Router# show ipv6 cef switching statistics

Reason                               Drop      Punt  Punt2Host
RP LES Packet destined for us        0      132248      0
RP LES Multicast                      0         2      0
RP LES Link-local                     0        33      0
RP LES Total                          0     132283      0

Slot 4 Packet destined for us        0     129546      0
Slot 4 Link-local                     0         31      0
Slot 4 Total                          0     129577      0

All   Total                          0     261860      0
```

[Table 94](#) describes the significant fields shown in the display.

Table 94 *show ipv6 cef switching statistics Field Descriptions*

| Field | Description |
|--------------|----------------------------|
| Reason | Packet description. |
| Drop | Number of packets dropped. |

Table 94 *show ipv6 cef switching statistics Field Descriptions (continued)*

| Field | Description |
|-----------|---|
| Punt | Number of packets that could be switched in the normal path and were punted to the next fastest switching vector. |
| Punt2Host | Number of packets that cannot be switched in the normal path and were punted to the host. |

Related Commands

| Command | Description |
|---------------------------|--|
| show cef interface | Displays Cisco Express Forwarding-related interface information. |
| show ipv6 cef | Displays entries in the IPv6 FIB. |
| show ipv6 route | Displays IPv6 router advertisement information received from onlink routers. |

show ipv6 cef traffic prefix-length

To display Cisco Express Forwarding for IPv6 (CEFv6) and distributed CEFv6 (dCEFv6) traffic statistics, use the **show ipv6 cef traffic prefix-length** command in user EXEC or privileged EXEC mode.

show ipv6 cef traffic prefix-length

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC

Command History

| Release | Modification |
|-------------|---|
| 12.0(22)S | This command was introduced. |
| 12.2(13)T | This command was integrated into 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(28)SB | This command was integrated into Cisco IOS Release 12.2(28)SB. |
| 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(20)T | This command was integrated into Cisco IOS Release 12.4(20)T. |

Usage Guidelines

The **show ipv6 cef traffic prefix-length** command is similar to the **show ip cef traffic prefix-length** command, except that it is IPv6-specific.

This command is used to display CEFv6 switched traffic statistics by destination prefix length. The **ipv6 cef accounting prefix-length** command must be enabled for the counters to increment.

Examples

The following is sample output from the **show ipv6 cef traffic prefix-length** command:

```
Router# show ipv6 cef traffic prefix-length
```

```
IPv6 prefix length switching statistics:
```

```
-----
Prefix      Number of      Number of
Length      Packets        Bytes
-----
          0              0              0
          1             24             3840
          2              0              0
          3             14             1120
          4              0              0
          5             10             1200
          .
          .
          .
          28              0              0
```

| | | |
|----|----|------|
| 29 | 4 | 512 |
| 30 | 0 | 0 |
| 31 | 18 | 2448 |
| 32 | 0 | 0 |

Table 95 describes the significant fields shown in the display.

Table 95 *show ipv6 cef traffic prefix-length Field Descriptions*

| Field | Description |
|-------------------|---|
| Prefix Length | Destination IPv6 prefix length for Cisco Express Forwarding switched traffic. |
| Number of Packets | Number of packets forwarded for the specified IPv6 prefix length. |
| Number of Bytes | Number of bytes sent for the specified IPv6 prefix length. |

Related Commands

| Command | Description |
|------------------------------|--|
| ipv6 cef accounting | Enables CEFv6 network accounting. |
| show ipv6 cef | Displays entries in the IPv6 FIB. |
| show ipv6 cef summary | Displays a summary of the entries in the IPv6 FIB. |

show ipv6 cef tree

To display summary information on the default tree in the IPv6 Forwarding Information Base (FIB), use the **show ipv6 cef tree** command in user EXEC or privileged EXEC mode.

show ipv6 cef tree [**statistics** | **dependents** [*prefix-filter*]]

| Syntax Description | | |
|----------------------|------------|---|
| statistics | (Optional) | Displays the default tree statistics. |
| dependents | (Optional) | Displays the dependents of the selected tree with optional prefix filter. |
| <i>prefix-filter</i> | (Optional) | A prefix filter on the dependents of the selected tree. |

| Command Modes | |
|---------------|------------------------------|
| | User EXEC Privileged EXEC |

| Command History | Release | Modification |
|-----------------|-------------|---|
| | 12.2(25)S | This command was introduced. |
| | 12.2(28)SB | This command was integrated into Cisco IOS Release 12.2(28)SB. |
| | 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 | |
|------------------|--|
| | If none of the optional keywords or arguments is used, all summary information on the default tree in the IPv6 FIB is shown. |

Examples The following is sample output from the **show ipv6 cef tree** command:

```
Router# show ipv6 cef tree

VRF Default tree information:
RTRIE storing IPv6 addresses
6 entries (6/0 fwd/non-fwd)
Forwarding & Non-forwarding tree:
6 inserts, 0 delete
8 nodes using 288 bytes
```

[Table 96](#) describes the significant fields shown in the display.

Table 96 *show ipv6 cef tree* Field Descriptions

| Field | Description |
|------------------------------|---|
| RTRIE storing IPv6 addresses | Indicates the tree type as RTRIE. |
| 6 entries (6/0 fwd/non-fwd) | Indicates total number of prefix entries as 6 forwarding and 0 nonforwarding entries. |

Table 96 *show ipv6 cef tree Field Descriptions (continued)*

| Field | Description |
|--------------------------------------|---|
| Forwarding & Non-forwarding tree | Same tree is used for forwarding and nonforwarding. |
| 6 inserts, 0 delete | Indicates that 6 entries were inserted and 0 entries were deleted from the tree. |
| 8 nodes using 288 bytes | Indicates a total of 8 nodes using a total of 288 bytes of memory. |
| *calloc failures: <i>number</i> node | This line is not present in the example output. If this line is present in output, it indicates a memory allocation error at the indicated node. |

Related Commands

| Command | Description |
|----------------------|-----------------------------------|
| show ipv6 cef | Displays entries in the IPv6 FIB. |

show ipv6 cef unresolved

To display unresolved entries in the IPv6 Forwarding Information Base (FIB), use the **show ipv6 cef unresolved** command in user EXEC or privileged EXEC mode.

```
show ipv6 cef unresolved [detail | internal | samecable] [platform [detail | internal | samecable]]
[source [internal | epoch epoch-number [internal | samecable | platform [detail | internal |
samecable]]]] [epoch epoch-number [internal | samecable | platform [detail | internal |
samecable]]]
```

Syntax Description

| | |
|----------------------------------|--|
| detail | (Optional) Displays detailed FIB entry information. |
| internal | (Optional) Displays data structures for unresolved routes. |
| samecable | (Optional) Displays the connected (up) interface for unresolved routes. |
| platform | (Optional) Displays platform-specific information on unresolved routes. |
| source | (Optional) Displays source-specific information on unresolved routes. |
| epoch <i>epoch-number</i> | (Optional) Displays the basic unresolved routes filtered by a specified epoch number. The epoch number range is from 0 to 255. |

Command Modes

User EXEC
Privileged EXEC

Command History

| Release | Modification |
|-------------|--|
| 12.0(22)S | This command was introduced. |
| 12.2(13)T | This command was integrated into 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(25)S | The internal , samecable , platform , source , and epoch keywords were added. The <i>epoch-number</i> argument was added. |
| 12.2(28)SB | This command was integrated into Cisco IOS Release 12.2(28)SB. |
| 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(20)T | This command was integrated into Cisco IOS Release 12.4(20)T. |

Usage Guidelines

The **show ipv6 cef unresolved** command is similar to the **show ip cef unresolved** command, except that it is IPv6-specific.

The **show ipv6 cef unresolved detail** command displays detailed information for all unresolved FIB entries.

Examples

The following is sample output from the **show ipv6 cef unresolved** command with the **detail** keyword:

```
Router# show ipv6 cef unresolved detail

IPv6 CEF is enabled for distributed and running
VRF Default:
 5 prefixes (5/0 fwd/non-fwd)
Table id 0, version 5, 0 resets
Database epoch: 2 (5 entries at this epoch)
```

[Table 79](#) describes the significant fields shown in the display.

Table 97 *show ipv6 cef unresolved Field Descriptions*

| Field | Description |
|---|---|
| 5 prefixes (5/0 fwd/non-fwd) | Indicates how many IPv6 prefixes are being used for forwarding or not forwarding. |
| Table id 0, version 5, 0 resets | Provides information about the Cisco Express Forwarding table. |
| Database epoch: 2 (5 entries at this epoch) | The epoch number of any unresolved database epochs. |

This is an example of the **show ipv6 cef unresolved detail** command output in Cisco IOS Releases 12.2(25)S, 12.2(28)SB, 12.2(33)SRA, 12.2(33)SXH, 12.4(20)T, and later releases:

```
Router# show ipv6 cef unresolved detail
```

No unresolved adjacencies exist, therefore nothing is displayed in the output of the **show ipv6 cef unresolved detail** command.

Related Commands

| Command | Description |
|------------------------------|--|
| show cef interface | Displays Cisco Express Forwarding-related interface information. |
| show ipv6 cef | Displays entries in the IPv6 FIB. |
| show ipv6 cef summary | Displays a summary of the entries in the IPv6 FIB. |

show ipv6 cef vrf

To display the Cisco Express Forwarding Forwarding Information Base (FIB) associated with an IPv6 Virtual Private Network (VPN) routing and forwarding (VRF) instance, use the **show ipv6 cef vrf** command in user EXEC or privileged EXEC mode.

```
show ipv6 cef vrf [vrf-name | * | internal]
```

Syntax Description

| | |
|-----------------|---|
| <i>vrf-name</i> | (Optional) Name assigned to the VRF. |
| * | (Optional) All VRFs are displayed. |
| internal | (Optional) Only internal data is displayed. |

Command Modes

User EXEC
Privileged EXEC

Command History

| Release | Modification |
|--------------|--|
| 12.2(33)SRB | This command was introduced. |
| 12.2(33)SRB1 | This command was integrated into Cisco IOS Release 12.2(33)SRB1. |
| 12.2(33)SXH | This command was integrated into Cisco IOS Release 12.2(33)SXH. |
| 12.2(33)SB | This command was integrated into Cisco IOS Release 12.2(33)SB. |

Usage Guidelines

Use the **show ipv6 cef vrf** command to display content of the IPv6 FIB for the specified VRF.

Examples

The following is sample output from a Cisco Express Forwarding FIB associated with a VRF named `cisco1`:

```
Router# show ipv6 cef vrf cisco1

2001:8::/64
  attached to FastEthernet0/0
2001:8::3/128
  receive
2002:8::/64
  nexthop 10.1.1.2 POS4/0 label 22 19
2010::/64
  nexthop 2001:8::1 FastEthernet0/0
2012::/64
  attached to Loopback1
2012::1/128
  receive
```

[Table 98](#) describes the significant fields shown in the display.

Table 98 *show ipv6 cef vrf Field Descriptions*

| Field | Description |
|-------------------------------------|-------------------------------------|
| 2001:8::/64 | Specifies the network prefix. |
| attached to FastEthernet0/0 | Specifies the VRF interface. |
| nexthop 10.1.1.2 POS4/0 label 22 19 | Specifies the BGP next hop address. |

show ipv6 cef with epoch

To display Cisco Express Forwarding IPv6 Forwarding Information Base (FIB) information filtered for a specific epoch, use the **show ipv6 cef with epoch** command in privileged EXEC mode.

show ipv6 cef with epoch *epoch-number* [**checksum** | **detail** | **internal** [**checksum**] | **platform** [**checksum** | **detail** | **internal** [**checksum**]]]

Syntax Description

| | |
|---------------------|--|
| <i>epoch-number</i> | Number of the epoch, from 0 to 255. |
| checksum | (Optional) Displays FIB entry checksums. |
| detail | (Optional) Displays detailed information about FIB epochs. |
| internal | (Optional) Displays internal data structure information. |
| platform | (Optional) Displays platform-specific data structures. |

Command Modes

Privileged EXEC (#)

Command History

| Release | Modification |
|-------------|---|
| 12.2(25)S | This command was introduced. |
| 12.2(28)SB | This command was integrated into Cisco IOS Release 12.2(28)SB. |
| 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(20)T | This command was integrated into Cisco IOS Release 12.4(20)T. |

Usage Guidelines

Use this command to display information about prefix properties for a specified epoch in the Cisco Express Forwarding IPv6 FIB. This command is similar to the **show ip cef with epoch** command, except that it is IPv6 specific. Use the **show ipv6 cef epoch** command to display entries filtered by epoch number.

Examples

The following is sample output from the **show ipv6 cef with epoch** command:

```
Router# show ipv6 cef with epoch 0

::/0
  no route
::/127
  discard
2000::1/128
  receive for Loopback0
2000::2/128
  nexthop FE80::A8BB:CCFF:FE00:2500 Ethernet0/0
2000::3/128
  nexthop FE80::A8BB:CCFF:FE00:2602 Ethernet2/0
2000::4/128
  nexthop FE80::A8BB:CCFF:FE00:2602 Ethernet2/0
2001::/64
```

```

    attached to Ethernet2/0
2001::1/128
    receive for Ethernet2/0
2001::3/128
    attached to Ethernet2/0
2001:1::/64
    attached to Ethernet0/0
2001:1::1/128
    receive for Ethernet0/0
2001:2::/64
    nexthop FE80::A8BB:CCFF:FE00:2602 Ethernet2/0
2002::/64
    attached to Tunnel0
2002::1/128
    receive for Tunnel0
FE80::/10
    receive for Null0
FF00::/8
    receive for Null0

```

Table 99 describes significant fields shown in the display.

Table 99 *show ipv6 cef with epoch Field Descriptions*

| Field | Description |
|--|--|
| no route | No route is associated with the IPv6 prefix. |
| discard | Traffic for this prefix is discarded. |
| 2000::1/128 receive for Loopback0 | A receive prefix for interface Loopback0. |
| 2000::2/128 nexthop FE80::A8BB:CCFF:FE00:2500 Ethernet0/0 | An IPv6 prefix that is forwarded to a next-hop address (FE80::A8BB:CCFF:FE00:2500) through interface Ethernet 0/0. |
| 2001::/64 attached for Ethernet2/0 | This prefix is a connected network on interface Ethernet 0/0. |
| 2001::1/128 receive for Ethernet2/0 | A receive prefix for interface Ethernet 0/0. |

The following is sample output from the **show ipv6 cef with epoch detail** command:

```

Router# show ipv6 cef with epoch 0 detail

IPv6 CEF is enabled and running centrally.
VRF base:
 16 prefixes (16/0 fwd/non-fwd)
Table id 0
Database epoch:          0 (16 entries at this epoch)

::/0, epoch 0, flags default route handler
no route
::/127, epoch 0, flags attached, discard
discard
2000::1/128, epoch 0, flags attached, connected, receive, local
receive for Loopback0
2000::2/128, epoch 0
nexthop FE80::A8BB:CCFF:FE00:2500 Ethernet0/0
2000::3/128, epoch 0, flags rib only nolabel, rib defined all labels

```

```

nexthop FE80::A8BB:CCFF:FE00:2602 Ethernet2/0
2000::4/128, epoch 0, flags rib only nolabel, rib defined all labels
  nexthop FE80::A8BB:CCFF:FE00:2602 Ethernet2/0
2001::/64, epoch 0, flags attached, connected, cover dependents
  Covered dependent prefixes: 1
    notify cover updated: 1
    attached to Ethernet2/0
2001::1/128, epoch 0, flags attached, receive, local
  receive for Ethernet2/0
2001::3/128, epoch 0, flags attached
  Adj source: IPV6 adj out of Ethernet2/0, addr 2001::3 02513FD8
  Dependent covered prefix type adjfib cover 2001::/64
  attached to Ethernet2/0
2001:1::/64, epoch 0, flags attached, connected
  attached to Ethernet0/0
2001:1::1/128, epoch 0, flags attached, receive, local
  receive for Ethernet0/0
2001:2::/64, epoch 0, flags rib only nolabel, rib defined all labels
  nexthop FE80::A8BB:CCFF:FE00:2602 Ethernet2/0
2002::/64, epoch 0, flags attached, connected
  attached to Tunnel0
2002::1/128, epoch 0, flags attached, receive, local
  receive for Tunnel0
FE80::/10, epoch 0, flags attached, receive, local
  receive for Null0
FF00::/8, epoch 0, flags attached, receive, local
  receive for Null0

```

Table 100 describes significant fields shown in the display.

Table 100 show ipv6 cef with epoch detail Field Descriptions

| Field | Description |
|--|--|
| IPv6 CEF is enabled and running centrally | Indicates that IPv6 CEF is enabled and running on the RP. |
| VRF base 16 prefixes (16/0 fwd/non-fwd) | Number of prefixes in the VRF, how many of them are forwarded, and how many are not forwarded. |
| Table id 0 | Table identification number. |
| Database epoch 0 (16 entries at this epoch) | Value of the database epoch and number of entries in the epoch. |
| 2000::1/128, epoch 0, flags attached, connected, receive, local receive for Loopback0 | Provides detail for the table entries. In this example, 2000:1/128 is an IPv6 prefix at epoch 0. The flags set for this prefix are: <ul style="list-style-type: none"> attached—Prefix is a connected network connected—Prefix includes an address that is bound to an interface on the device receive—Prefix is punt to and handled by the process level local—Prefix is a subset of receive and marks prefixes that are received by on interface on the device |

The following is sample output from the **show ipv6 cef with epoch checksum** command:

```
Router# show ipv6 cef with epoch 0 checksum
```

```
::/0
  FIB checksum: 0x64E25610
::/127
  FIB checksum: 0xE0B3DE11
2000::1/128
  FIB checksum: 0xD04E36EC
2000::2/128
  FIB checksum: 0x84892BA5
2000::3/128
  FIB checksum: 0x912BA720
2000::4/128
  FIB checksum: 0xC6D89ADA
.
.
.
```

[Table 101](#) describes significant fields shown in the display.

Table 101 *show ipv6 cef with epoch checksum Field Descriptions*

| Field | Description |
|--------------------------|--|
| ::/0 | Default route handler. ::/0 prefix matches all addresses. (::/128 prefix is an exact match for all zero addresses only.) |
| FIB checksum: 0x64E25610 | FIB checksum associated with the named prefix. |

Related Commands

| Command | Description |
|-------------------------------|--|
| show ip cef with epoch | Displays Cisco Express Forwarding FIB information filtered for a specific epoch. |
| show ipv6 cef | Displays entries in the IPv6 FIB. |
| show ipv6 cef epoch | Displays a summary of IPv6 FIB epoch information. |

show ipv6 cef with source

To display Cisco Express Forwarding IPv6 Forwarding Information Base (FIB) filtered for a specific source, use the **show ipv6 cef with source** command in privileged EXEC mode.

```
show ipv6 cef with source source-type [checksum | detail | epoch | internal [checksum] |
platform [checksum | detail | internal [checksum]]]
```

Syntax Description

source-type

The *source-type* argument must be replaced by one of the following keywords that are supported for your release.

Keywords for all supported Cisco IOS releases:

- **alias**—Displays alias address prefix sources in the Cisco Express Forwarding IPv6 FIB.
- **broadband**—Displays broadband receive prefix sources in the Cisco Express Forwarding IPv6 FIB.
- **fallback**—Displays fallback lookup prefix sources in the Cisco Express Forwarding IPv6 FIB.
- **interface**—Displays interface configuration prefix sources in the Cisco Express Forwarding IPv6 FIB.
- **nat**—Displays Network Address Translation (NAT) prefix sources in the Cisco Express Forwarding IPv6 FIB.
- **rib**—Displays Routing Information Base (RIB) prefix sources in the Cisco Express Forwarding IPv6 FIB.
- **special**—Displays special prefix sources in the Cisco Express Forwarding IPv6 FIB.
- **test**—Displays test command prefix sources in the Cisco Express Forwarding IPv6 FIB.
- **virtual**—Displays virtual address prefix sources in the Cisco Express Forwarding IPv6 FIB, for example, Virtual Router Redundancy Protocol (VRRP) and Hot Standby Router Protocol (HSRP) addresses.

Additional keywords for Cisco IOS Releases 12.2(25)S, 12.2(28)SB, 12.2(33)SRA, and later SB and SR releases:

- **adjacency**—Displays adjacency prefix sources in the Cisco Express Forwarding IPv6 FIB.
- **default-route**—Displays default route handler prefix sources in the Cisco Express Forwarding IPv6 FIB.
- **inherited-path-list**—Displays inherited path list prefix source in the Cisco Express Forwarding IPv6 FIB.

Additional keywords for Cisco IOS Releases 12.2(33)SXH, 12.4(20)T, and later SX and T releases:

- **adj**—Displays adjacency prefix sources in the Cisco Express Forwarding IPv6 FIB.

- **defnet**—Displays default network prefix sources in the Cisco Express Forwarding IPv6 FIB.
- **defroutehandler**—Displays default route handler prefix sources in the Cisco Express Forwarding IPv6 FIB.
- **ipl**—Displays inherited path list prefix source in the Cisco Express Forwarding IPv6 FIB.

Additional keywords for Cisco IOS Releases 12.2(33)SRA, 12.2(33)SXH and later SR and SX releases:

- **recursive-resolution**—Displays recursive resolution prefix sources in the Cisco Express Forwarding IPv6 FIB.

Additional keyword for Cisco IOS Release 12.2(33)SXH and later SX releases:

- **lte**—Displays Multiprotocol Label Switching (MPLS) label table entries.

| | |
|-----------------|---|
| checksum | (Optional) Displays IPv6 FIB entry checksums. |
| detail | (Optional) Displays detailed information about IPv6 FIB epochs. |
| epoch | (Optional) Displays information about epochs associated with the source prefix. |
| internal | (Optional) Displays internal data structure information. |
| platform | (Optional) Displays platform-specific data structures. |

Command Modes

Privileged EXEC (#)

Command History

| Release | Modification |
|-------------|---|
| 12.2(25)S | This command was introduced. |
| 12.2(28)SB | This command was integrated into Cisco IOS Release 12.2(28)SB. |
| 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(20)T | This command was integrated into Cisco IOS Release 12.4(20)T. |

Usage Guidelines

Use this command to filter on prefixes in the Cisco Express Forwarding FIB that are added by a specified source.

Examples

Examples For All Supported Releases

The following is sample output from the **show ipv6 cef with source rib** command:

```
Router# show ipv6 cef with source rib

::/127
  discard
2000::1/128
  receive for Loopback0
2000::2/128
```

```

    nexthop FE80::A8BB:CCFF:FE00:2500 Ethernet0/0
2000::3/128
    nexthop FE80::A8BB:CCFF:FE00:2602 Ethernet2/0
2000::4/128
    nexthop FE80::A8BB:CCFF:FE00:2602 Ethernet2/0
2001::/64
    attached to Ethernet2/0
2001::1/128
    receive for Ethernet2/0
2001:1::/64
    attached to Ethernet0/0
2001:1::1/128
    receive for Ethernet0/0
2001:2::/64
    nexthop FE80::A8BB:CCFF:FE00:2602 Ethernet2/0
2002::/64
    attached to Tunnel0
2002::1/128
    receive for Tunnel0
FE80::/10
    receive for Null0
FF00::/8
    receive for Null0

```

Table 102 describes the significant fields shown in the display.

Table 102 show ipv6 cef with source rib Field Descriptions

| Field | Description |
|--|---|
| ::/127 | IPv6 prefix. |
| discard | Indicates that traffic destined for this prefix should be discarded. |
| 2000::1/128 receive for Loopback0 | An IPv6 prefix that is a receive prefix for interface Loopback0. Traffic destined for this prefix will be punted to the process level. |
| 2000::2/128 nexthop FE80::A8BB:CCFF:FE00:2500 Ethernet0/0 | An IPv6 prefix that is forwarded to a next-hop address (FE80::A8BB:CCFF:FE00:2500) through interface Ethernet 0/0. |
| 2001::/64 attached for Ethernet2/0 | An IPv6 prefix that is a connected network on interface Ethernet 0/0. That is, the destination can be reached directly through the specified interface. |

The following is sample output from the **show ipv6 cef with source fib detail** command:

```

Router# show ipv6 cef with source rib detail

IPv6 CEF is enabled and running centrally.
VRF base:
 16 prefixes (16/0 fwd/non-fwd)
Table id 0
Database epoch:          0 (16 entries at this epoch)

::/127, epoch 0, flags attached, discard
  discard
2000::1/128, epoch 0, flags attached, connected, receive, local
  receive for Loopback0
2000::2/128, epoch 0
  nexthop FE80::A8BB:CCFF:FE00:2500 Ethernet0/0
2000::3/128, epoch 0, flags rib only nolabel, rib defined all labels

```

```

nexthop FE80::A8BB:CCFF:FE00:2602 Ethernet2/0
2000::4/128, epoch 0, flags rib only nolabel, rib defined all labels
nexthop FE80::A8BB:CCFF:FE00:2602 Ethernet2/0
2001::/64, epoch 0, flags attached, connected, cover dependents
  Covered dependent prefixes: 1
    notify cover updated: 1
    attached to Ethernet2/0
2001::1/128, epoch 0, flags attached, receive, local
  receive for Ethernet2/0
2001:1::/64, epoch 0, flags attached, connected
  attached to Ethernet0/0
2001:1::1/128, epoch 0, flags attached, receive, local
  receive for Ethernet0/0
2001:2::/64, epoch 0, flags rib only nolabel, rib defined all labels
nexthop FE80::A8BB:CCFF:FE00:2602 Ethernet2/0
2002::/64, epoch 0, flags attached, connected
  attached to Tunnel0
2002::1/128, epoch 0, flags attached, receive, local
  receive for Tunnel0
FE80::/10, epoch 0, flags attached, receive, local
  receive for Null0
FF00::/8, epoch 0, flags attached, receive, local
  receive for Null0

```

Table 103 describes the significant fields shown in the display.

Table 103 *show ipv6 cef with source rib detail Field Descriptions*

| Field | Description |
|---|--|
| IPv6 CEF is enabled and running centrally. | Verifies that Cisco Express Forwarding for IPV6 is enabled globally. |
| VRF base | Base VRF table. |
| 16 prefixes (16/0 Fwd/non-fwd) | Number of prefixes in the VRF, how many prefixes are forwarded, and how many are not forwarded. |
| Table id 0 | Identifies the table by number. |
| Database epoch: | Specifies the type of epoch. |
| 0 (16 entries at this epoch) | Number of the epoch (0) and number of entries in the epoch. |
| 2000::1/128, epoch 0, flags attached, connected, receive, local | Details about the prefix: the epoch in which it is found, the flags set for the prefix: <ul style="list-style-type: none"> • attached—Prefix is a connected network • connected—Prefix includes an address that is bound to an interface on the device • receive—Prefix is punt to and handled by the process level • local—Prefix is a subset of receive and marks prefixes that are received by on interface on the device |

Examples for Cisco IOS Releases 12.2(25)S, 12.2(28)SB, 12.2(33)SRA, and Later SB and SR Releases

The following is sample output from the **show ipv6 cef with source adjacency** command:

```
Router# show ipv6 cef with source adjacency
```

```
2001::3/128
  attached to Ethernet2/0
```

Table 104 describes the significant fields shown in the display.

Table 104 show ipv6 cef with source adjacency Field Descriptions

| Field | Description |
|-------------------------|--|
| 2001::3/128 | IPv6 prefix whose source is an adjacency. |
| attached to Ethernet2/0 | Indicates that the prefix is a connected network through Interface Ethernet 2/0. |

The following is sample output from the **show ipv6 cef with source adjacency detail** command:

```
Router# show ipv6 cef with source adjacency detail
#
IPv6 CEF is enabled and running centrally.
VRF Default
 16 prefixes (16/0 fwd/non-fwd)
Table id 0x1E000000
Database epoch:          0 (16 entries at this epoch)

2001::3/128, epoch 0, flags attached
  Adj source: IPV6 adj out of Ethernet2/0, addr 2001::3 050878F0
  Dependent covered prefix type adjfib cover 2001::/64
  attached to Ethernet2/0
```

Table 105 describes the significant fields shown in the display.

Table 105 show ipv6 cef with source adjacency detail Field Descriptions

| Field | Description |
|--|--|
| IPv6 CEF is enabled and running centrally. | Verifies that Cisco Express Forwarding for IPV6 is enabled and running on the RP. |
| VRF Default | Default VRF table. |
| 16 prefixes (16/0 Fwd/non-fwd) | Number of prefixes in the VRF, how many prefixes are forwarded and how many are not forwarded. |
| Table id 0x1E000000 | Identifies the table by hexadecimal number. |
| 2001::3/128, epoch 0, flags attached | Lists a prefix, its epoch number, and flags. Attached flag indicates a connected network. |
| Adj source: IPv6 adj out of Ethernet2/0, addr 2000::3 050878F0 | Indicates that the prefix was sourced by an adjacency and specifies the address family, interface, and address in memory of the adjacency. |

Table 105 show ipv6 cef with source adjacency detail Field Descriptions (continued)

| Field | Description |
|---|--|
| Dependent covered prefix type adjfib cover 2001::/64 | A prefix sourced by an adjacency is dependent on another less specific prefix (2001::/64) for forwarding information. If this less specific prefix changes, the dependent prefix will need to be recomputed. |
| attached to Ethernet2/0 | Indicates the prefix is a connect network through interface Ethernet 2/0. |

The following is sample output from the **show ipv6 cef with source adjacency checksum** command:

```
Router# show ipv6 cef with source adjacency checksum
```

```
2001::3/128
  FIB checksum: 0x4AE0F5DC
```

[Table 106](#) describes the significant fields shown in the display.

Table 106 show ipv6 cef with source adjacency checksum Field Descriptions

| Field | Description |
|--------------------------|---|
| 2001::3/128 | IPv6 prefix whose source is an adjacency. |
| FIB checksum: 0x4AE0F5DC | FIB checksum. |

Examples for Cisco IOS Releases 12.2(33)SXH, 12.4(20)T and Later SX and T Releases

The following is sample output from the **show ipv6 cef with source adjacency** command:

```
Router# show ipv6 cef with source adj
```

```
2001::3/128
  attached to Ethernet2/0
```

[Table 107](#) describes the significant fields shown in the display.

Table 107 show ipv6 cef with source adj Field Descriptions

| Field | Description |
|-------------------------|--|
| 2001::3/128 | IPv6 prefix whose source is an adjacency. |
| attached to Ethernet2/0 | Indicates that the prefix is a network connected through interface Ethernet 2/0. |

The following is sample output from the **show ipv6 cef with source adj detail** command:

```
Router# show ipv6 cef with source adj detail
```

```
IPv6 CEF is enabled and running centrally.
VRF base:
  16 prefixes (16/0 fwd/non-fwd)
  Table id 0
  Database epoch:          0 (16 entries at this epoch)

2001::3/128, epoch 0, flags attached
  Adj source: IPV6 adj out of Ethernet2/0, addr 2001::3 02513FD8
```

show ipv6 cef with source

```
Dependent covered prefix type adjfib cover 2001::/64
attached to Ethernet2/0
```

Table 108 describes the significant fields shown in the display.

Table 108 *show ipv6 cef with source adj detail Field Descriptions*

| Field | Description |
|--|--|
| IPv6 CEF is enabled and running centrally. | Verifies that Cisco Express Forwarding for IPv6 is enabled and running on the RP. |
| VRF base | Base VRF table. |
| 16 prefixes (16/0 Fwd/non-fwd) | Number of prefixes, and how many prefixes are forwarded and how many are not forwarded. |
| 2001::3/128, epoch 0, flags attached | Provides more detail about the adjacency source, such as epoch number and flags. |
| Adj source: IPv6 adj out of Ethernet2/0, addr 2000::3 050878F0 | Lists a prefix, its epoch number, and flags. Attached flag indicates a connected network. |
| Dependent covered prefix type adjfib cover 2001::/64 | A prefix sourced by an adjacency is dependent on another less specific prefix (2001::/64) for forwarding information. If this less specific prefix changes, the dependent prefix will need to be recomputed. |
| attached to Ethernet2/0 | Indicates the prefix is a connected network through interface Ethernet 2/0. |

The following is sample output from the **show ipv6 cef with source adj checksum** command:

```
Router# show ipv6 cef with source adj checksum
2001::3/128
  FIB checksum: 0x4AE0F5DC
```

Table 109 describes the significant fields shown in the display.

Table 109 *show ipv6 cef with source adj checksum Field Descriptions*

| Field | Description |
|--------------------------|---|
| 2001::3/128 | IPv6 prefix whose source is an adjacency. |
| FIB checksum: 0x4AE0F5DC | FIB checksum. |

Related Commands

| Command | Description |
|----------------------------------|---|
| show ip cef | Displays entries in the FIB or displays a summary of the FIB. |
| show ip cef with epoch | Displays information about an epoch in the Cisco Express Forwarding FIB. |
| show ipv6 cef with epoch | Displays information about an epoch in the Cisco Express Forwarding IPv6 FIB. |
| show ipv6 cef with source | Displays information about prefix sources in the Cisco Express Forwarding IPv6 FIB. |

show ipv6 cga address-db

To display IPv6 cryptographically generated addresses (CGA) from the address database, use the **show ipv6 cga address-db** command in privileged EXEC mode.

```
show ipv6 cga address-db
```

Syntax Description This command has no arguments or keywords.

Command Default No CGAs are displayed.

Command Modes Privileged EXEC

| Command History | Release | Modification |
|-----------------|-----------|------------------------------|
| | 12.4(24)T | This command was introduced. |

Examples The following example displays CGAs in the CGA database:

```
Router# show ipv6 cga address-db

2001:0DB8:/64 ::2011:B680:DEF4:A550 - table 0x0
  interface:      Ethernet0/0 (3)
  modifier:       SEND1024e
FE80::/64 ::3824:3CE4:C044:8D65 - table 0x12000003
  interface:      Ethernet0/0 (3)
  modifier:       SEND1024e
```

[Table 110](#) describes the significant fields shown in the display.

Table 110 *show ipv6 cga address-db Field Descriptions*

| Field | Description |
|---|---|
| 2001:0DB8:/64 ::2011:B680:DEF4:A550 - table 0x0 | CGA address for which information is shown. |
| interface: | Interface on which the address is configured. |
| modifier: | The CGA modifier. |

| Related Commands | Command | Description |
|------------------|--|---|
| | show ipv6 cga modifier-db | Displays IPv6 CGA modifiers. |
| | show ipv6 nd secured certificates | Displays active SeND certificates. |
| | show ipv6 nd secured counters interface | Displays SeND counters on an interface. |

show ipv6 cga address-db

| Command | Description |
|--|--|
| show ipv6 nd secured nonce-db | Displays active SeND nonce entries. |
| show ipv6 nd secured timestamp-db | Displays active SeND time-stamp entries. |

show ipv6 cga modifier-db

To display IPv6 cryptographically generated address (CGA) modifier database entries, use the **show ipv6 cga modifier-db** command in privileged EXEC mode.

```
show ipv6 cga modifier-db
```

Syntax Description This command has no arguments or keywords.

Command Default No CGA modifiers are displayed.

Command Modes Privileged EXEC

| Command History | Release | Modification |
|-----------------|-----------|------------------------------|
| | 12.4(24)T | This command was introduced. |

Usage Guidelines The **show ipv6 cga modifier-db** command is used to display the modifiers generated with the **ipv6 cga modifier** command and the addresses generated from them.

Examples The following example displays CGA modifiers in the CGA modifier database:

```
Router# show ipv6 cga modifier-db

F046:E042:13E8:1661:96E5:DD05:94A8:FADC
  label:          SubCA11
  sec level:      1
  Addresses:
  2001:100::38C9:4A1A:2972:794E
  FE80::289C:3308:4719:87F2
```

[Table 110](#) describes the significant fields shown in the display.

Table 111 *show ipv6 cga modifier-db Field Descriptions*

| Field | Description |
|--|---|
| D695:5D75:F9B5:9715:DF0A: D840:70A2:84B8 | The CGA modifier for which the information is displayed. |
| label | Name used for the Rivest, Shamir, and Adelman (RSA) key pair. |
| Addresses: 2001:100::38C9:4A1A:2972:79 4EFE80::289C:3308:4719:87F2 | The CGA address. |

Related Commands

| Command | Description |
|--|--|
| ipv6 cga modifier | Generates an IPv6 CGA modifier for a specified RSA key pair. |
| show ipv6 cga address-db | Displays IPv6 CGAs. |
| show ipv6 nd secured certificates | Displays active SeND certificates. |
| show ipv6 nd secured counters interface | Displays SeND counters on an interface. |
| show ipv6 nd secured nonce-db | Displays active SeND nonce entries. |
| show ipv6 nd secured timestamp-db | Displays active SeND time-stamp entries. |

show ipv6 dhcp

To display the Dynamic Host Configuration Protocol (DHCP) unique identifier (DUID) on a specified device, use the **show ipv6 dhcp** command in user EXEC or privileged EXEC mode.

show ipv6 dhcp

Syntax Description This command has no arguments or keywords.

Command Modes User EXEC
Privileged EXEC

| Command History | Release | Modification |
|-----------------|--------------------------|--|
| | 12.3(4)T | This command was introduced. |
| | Cisco IOS XE Release 2.1 | This command was integrated into Cisco IOS XE Release 2.1. |
| | 12.2(33)SRE | This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE. |

Usage Guidelines The **show ipv6 dhcp** command uses the DUID based on the link-layer address for both client and server identifiers. The device uses the MAC address from the lowest-numbered interface to form the DUID. The network interface is assumed to be permanently attached to the device. Use the **show ipv6 dhcp** command to display the DUID of a device.

Examples The following is sample output from the **show ipv6 dhcp** command. The output is self-explanatory:

```
Router# show ipv6 dhcp
```

```
This device's DHCPv6 unique identifier(DUID): 000300010002FCA5DC1C
```


show ipv6 dhcp binding

To display automatic client bindings from the Dynamic Host Configuration Protocol (DHCP) for IPv6 server binding table, use the **show ipv6 dhcp binding** command in user EXEC or privileged EXEC mode.

```
show ipv6 dhcp binding [ipv6-address] [vrf vrf-name]
```

Syntax Description

| | |
|----------------------------|--|
| <i>ipv6-address</i> | (Optional) The address of a DHCP for IPv6 client. |
| vrf <i>vrf-name</i> | (Optional) Specifies a virtual routing and forwarding (VRF) configuration. |

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

| Release | Modification |
|---------------------------|--|
| 12.3(4)T | This command was introduced. |
| 12.4 | This command was modified. Command output was updated to display a PPP username associated with a binding. |
| 12.4(24)T | This command was modified. Command output was updated to display address bindings. |
| Cisco IOS XE Release 2.1 | This command was integrated into Cisco IOS XE Release 2.1. |
| 15.1(2)S | This command was modified. The vrf <i>vrf-name</i> keyword and argument were added. |
| Cisco IOS XE Release 3.3S | This command was modified. The vrf <i>vrf-name</i> keyword and argument were added. |

Usage Guidelines

The **show ipv6 dhcp binding** command displays all automatic client bindings from the DHCP for IPv6 server binding table if the *ipv6-address* argument is not specified. When the *ipv6-address* argument is specified, only the binding for the specified client is displayed.

If the **vrf** *vrf-name* keyword and argument combination is specified, all bindings that belong to the specified VRF are displayed.

Examples

The following sample output displays all automatic client bindings from the DHCP for IPv6 server binding table:

```
Router# show ipv6 dhcp binding

Client: FE80::A8BB:CCFF:FE00:300
DUID: 00030001AABBCC000300
Username : client_1
Interface: Virtual-Access2.1
IA PD: IA ID 0x000C0001, T1 75, T2 135
Prefix: 2001:380:E00::/64
```

```

        preferred lifetime 150, valid lifetime 300
        expires at Dec 06 2007 12:57 PM (262 seconds)
Client: FE80::A8BB:CCFF:FE00:300 (Virtual-Access2.2)
      DUID: 00030001AABBCC000300
      IA PD: IA ID 0x000D0001, T1 75, T2 135
        Prefix: 2001:0DB8:E00:1::/64
        preferred lifetime 150, valid lifetime 300
        expires at Dec 06 2007 12:58 PM (288 seconds)

```

Table 112 describes the significant fields shown in the display.

Table 112 *show ipv6 dhcp binding Field Descriptions*

| Field | Description |
|------------------------------------|--|
| Client | Address of a specified client. |
| DUID | DHCP unique identifier (DUID). |
| Virtual-Access2.1 | First virtual client. When an IPv6 DHCP client requests two prefixes with the same DUID but a different identity association for prefix delegation (IAPD) on two different interfaces, these prefixes are considered to be for two different clients, and interface information is maintained for both. |
| Username : client_1 | The username associated with the binding. |
| IA PD | Collection of prefixes assigned to a client. |
| IA ID | Identifier for this IAPD. |
| Prefix | Prefixes delegated to the indicated IAPD on the specified client. |
| preferred lifetime, valid lifetime | The preferred lifetime and valid lifetime settings, in seconds, for the specified client. |
| Expires at | Date and time at which the valid lifetime expires. |
| Virtual-Access2.2 | Second virtual client. When an IPv6 DHCP client requests two prefixes with the same DUID but different IAIDs on two different interfaces, these prefixes are considered to be for two different clients, and interface information is maintained for both. |

When the DHCPv6 pool on the Cisco IOS DHCPv6 server is configured to obtain prefixes for delegation from an authentication, authorization, and accounting (AAA) server, it sends the PPP username from the incoming PPP session to the AAA server for obtaining the prefixes. The PPP username is associated with the binding is displayed in output from the **show ipv6 dhcp binding** command. If there is no PPP username associated with the binding, this field value is displayed as “unassigned.”

The following example shows that the PPP username associated with the binding is “client_1”:

```

Router# show ipv6 dhcp binding

Client: FE80::2AA:FF:FEBB:CC
      DUID: 0003000100AA00BB00CC
      Username : client_1
      Interface : Virtual-Access2
      IA PD: IA ID 0x00130001, T1 75, T2 135
        Prefix: 2001:0DB8:1:3::/80
        preferred lifetime 150, valid lifetime 300
        expires at Aug 07 2008 05:19 AM (225 seconds)

```

The following example shows that the PPP username associated with the binding is unassigned:

■ show ipv6 dhcp binding

```
Router# show ipv6 dhcp binding

Client: FE80::2AA:FF:FE8B:CC
DUID: 0003000100AA00BB00CC
Username : unassigned
Interface : Virtual-Access2
IA PD: IA ID 0x00130001, T1 150, T2 240
Prefix: 2001:0DB8:1:1::/80
        preferred lifetime 300, valid lifetime 300
        expires at Aug 11 2008 06:23 AM (233 seconds)
```

Related Commands

| Command | Description |
|--------------------------------|---|
| clear ipv6 dhcp binding | Deletes automatic client bindings from the DHCP for IPv6 binding table. |

show ipv6 dhcp conflict

To display address conflicts found by a Dynamic Host Configuration Protocol for IPv6 (DHCPv6) server when addresses are offered to the client, use the **show ipv6 dhcp conflict** command in privileged EXEC mode.

```
show ipv6 dhcp conflict [ipv6-address] [vrf vrf-name]
```

Syntax Description

| | |
|---------------------|--|
| <i>ipv6-address</i> | (Optional) The address of a DHCP for IPv6 client. |
| vrf vrf-name | (Optional) Specifies a virtual routing and forwarding (VRF) configuration. |

Command Modes

Privileged EXEC (#)

Command History

| Release | Modification |
|---------------------------|---|
| 12.4(24)T | This command was introduced. |
| Cisco IOS XE Release 2.5 | This command was integrated into Cisco IOS XE Release 2.5. |
| 15.1(2)S | This command was modified. The vrf vrf-name keyword and argument were added. |
| Cisco IOS XE Release 3.3S | This command was modified. The vrf vrf-name keyword and argument were added. |

Usage Guidelines

When you configure the DHCPv6 server to detect conflicts, it uses ping. The client uses neighbor discovery to detect clients and reports to the server through a DECLINE message. If an address conflict is detected, the address is removed from the pool, and the address is not assigned until the administrator removes the address from the conflict list.

Examples

The following is a sample output from the **show ipv6 dhcp conflict** command. This command shows the pool and prefix values for DHCP conflicts.:

```
Router# show ipv6 dhcp conflict
Pool 350, prefix 2001:0DB8:1005::/48
      2001:0DB8:1005::10
```

Related Commands

| Command | Description |
|---------------------------------|---|
| clear ipv6 dhcp conflict | Clears an address conflict from the DHCPv6 server database. |

show ipv6 dhcp database

To display the Dynamic Host Configuration Protocol (DHCP) for IPv6 binding database agent information, use the **show ipv6 dhcp database** command in user EXEC or privileged EXEC mode.

show ipv6 dhcp database [*agent-URL*]

Syntax Description

agent-URL (Optional) A flash, NVRAM, FTP, TFTP, or remote copy protocol (RCP) uniform resource locator.

Command Modes

User EXEC
Privileged EXEC

Command History

| Release | Modification |
|--------------------------|--|
| 12.3(4)T | This command was introduced. |
| Cisco IOS XE Release 2.1 | This command was integrated into Cisco IOS XE Release 2.1. |

Usage Guidelines

Each permanent storage to which the binding database is saved is called the database agent. An agent can be configured using the **ipv6 dhcp database** command. Supported database agents include FTP and TFTP servers, RCP, Flash file system, and NVRAM.

The **show ipv6 dhcp database** command displays DHCP for IPv6 binding database agent information. If the *agent-URL* argument is specified, only the specified agent is displayed. If the *agent-URL* argument is not specified, all database agents are shown.

Examples

The following is sample output from the **show ipv6 dhcp database** command:

```
Router# show ipv6 dhcp database

Database agent tftp://172.19.216.133/db.tftp:
  write delay: 69 seconds, transfer timeout: 300 seconds
  last written at Jan 09 2003 01:54 PM,
    write timer expires in 56 seconds
  last read at Jan 06 2003 05:41 PM
  successful read times 1
  failed read times 0
  successful write times 3172
  failed write times 2
Database agent nvrAM:/dhcpv6-binding:
  write delay: 60 seconds, transfer timeout: 300 seconds
  last written at Jan 09 2003 01:54 PM,
    write timer expires in 37 seconds
  last read at never
  successful read times 0
  failed read times 0
  successful write times 3325
  failed write times 0
Database agent flash:/dhcpv6-db:
```

```

write delay: 82 seconds, transfer timeout: 3 seconds
last written at Jan 09 2003 01:54 PM,
  write timer expires in 50 seconds
last read at never
successful read times 0
failed read times 0
successful write times 2220
failed write times 614

```

Table 113 describes the significant fields shown in the display.

Table 113 *show ipv6 dhcp database Field Descriptions*

| Field | Description |
|-------------------------------|--|
| Database agent | Specifies the database agent. |
| Write delay | The amount of time (in seconds) to wait before updating the database. |
| transfer timeout | Specifies how long (in seconds) the DHCP server should wait before aborting a database transfer. Transfers that exceed the timeout period are aborted. |
| Last written | The last date and time bindings were written to the file server. |
| Write timer expires... | The length of time, in seconds, before the write timer expires. |
| Last read | The last date and time bindings were read from the file server. |
| Successful/failed read times | The number of successful or failed read times. |
| Successful/failed write times | The number of successful or failed write times. |

Related Commands

| Command | Description |
|---------------------------|--|
| ipv6 dhcp database | Specifies DHCP for IPv6 binding database agent parameters. |

show ipv6 dhcp interface

To display Dynamic Host Configuration Protocol (DHCP) for IPv6 interface information, use the **show ipv6 dhcp interface** command in user EXEC or privileged EXEC mode.

```
show ipv6 dhcp interface [type number]
```

Syntax Description

| | |
|--------------------|---|
| <i>type number</i> | (Optional) Interface type and number. For more information, use the question mark (?) online help function. |
|--------------------|---|

Command Modes

User EXEC
Privileged EXEC

Command History

| Release | Modification |
|--------------------------|---|
| 12.3(4)T | This command was introduced. |
| 12.3(11)T | Command output was modified to allow relay agent information to be displayed on a specified interface if the relay agent feature is configured on that interface. |
| 12.4(24)T | Command output was updated to display interface address assignments and T1 and T2 renew/rebind times. |
| Cisco IOS XE Release 2.1 | This command was integrated into Cisco IOS XE Release 2.1. |
| 12.2(33)SRE | This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE. |
| 12.2(33)XNE | This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE. |

Usage Guidelines

If no interfaces are specified, all interfaces on which DHCP for IPv6 (client or server) is enabled are shown. If an interface is specified, only information about the specified interface is displayed.

Examples

The following is sample output from the **show ipv6 dhcp interface** command. In the first example, the command is used on a router that has an interface acting as a DHCP for IPv6 server. In the second example, the command is used on a router that has an interface acting as a DHCP for IPv6 client:

```
Router1# show ipv6 dhcp interface
```

```
Ethernet2/1 is in server mode
  Using pool: svr-pl
  Preference value: 20
  Rapid-Commit is disabled
```

```
Router2# show ipv6 dhcp interface
```

```
Ethernet2/1 is in client mode
  State is OPEN (1)
  List of known servers:
```

```

Address: FE80::202:FCFF:FEA1:7439, DUID 000300010002FCA17400
Preference: 20
  IA PD: IA ID 0x00040001, T1 120, T2 192
    Prefix: 3FFE:C00:C18:1::/72
      preferred lifetime 240, valid lifetime 54321
      expires at Nov 08 2002 09:10 AM (54319 seconds)
    Prefix: 3FFE:C00:C18:2::/72
      preferred lifetime 300, valid lifetime 54333
      expires at Nov 08 2002 09:11 AM (54331 seconds)
    Prefix: 3FFE:C00:C18:3::/72
      preferred lifetime 280, valid lifetime 51111
      expires at Nov 08 2002 08:17 AM (51109 seconds)
  DNS server: 1001::1
  DNS server: 1001::2
  Domain name: domain1.net
  Domain name: domain2.net
  Domain name: domain3.net
  Prefix name is cli-p1
  Rapid-Commit is enabled

```

Table 114 describes the significant fields shown in the display.

Table 114 *show ipv6 dhcp interface Field Descriptions*

| Field | Description |
|--------------------------------------|---|
| Ethernet2/1 is in server/client mode | Displays whether the specified interface is in server or client mode. |
| Preference value: | The advertised (or default of 0) preference value for the indicated server. |
| Prefix name is cli-p1 | Displays the IPv6 general prefix pool name, in which prefixes successfully acquired on this interface are stored. |
| Using pool: svr-p1 | The name of the pool that is being used by the interface. |
| State is OPEN | State of the DHCP for IPv6 client on this interface. "Open" indicates that configuration information has been received. |
| List of known servers | Lists the servers on the interface. |
| Address, DUID | Address and DHCP unique identifier (DUID) of a server heard on the specified interface. |
| Rapid commit is disabled | Displays whether the rapid-commit keyword has been enabled on the interface. |

The following example shows the DHCP for IPv6 relay agent configuration on FastEthernet interface 0/0, and use of the **show ipv6 dhcp interface** command displays relay agent information on FastEthernet interface 0/0:

```

Router(config-if)# ipv6 dhcp relay destination FE80::250:A2FF:FEBF:A056 FastEthernet0/1

Router# show ipv6 dhcp interface FastEthernet 0/0

FastEthernet0/0 is in relay mode
Relay destinations:
  FE80::250:A2FF:FEBF:A056 via FastEthernet0/1

```


| Related Commands | Command | Description |
|------------------|------------------------------------|--|
| | ipv6 dhcp client pd | Enables the DHCP for IPv6 client process and enables requests for prefix delegation through a specified interface. |
| | ipv6 dhcp relay destination | Specifies a destination address to which client messages are forwarded and enables DHCP for IPv6 relay service on the interface. |
| | ipv6 dhcp server | Enables DHCP for IPv6 service on an interface. |

show ipv6 dhcp pool

To display Dynamic Host Configuration Protocol (DHCP) for IPv6 configuration pool information, use the **show ipv6 dhcp pool** command in user EXEC or privileged EXEC mode.

```
show ipv6 dhcp pool [poolname]
```

| Syntax Description | <i>poolname</i> | (Optional) User-defined name for the local prefix pool. The pool name can be a symbolic string (such as “Engineering”) or an integer (such as 0). |
|--------------------|-----------------|---|
|--------------------|-----------------|---|

| Command Modes | User EXEC Privileged EXEC |
|---------------|------------------------------|
|---------------|------------------------------|

| Command History | Release | Modification |
|-----------------|--------------------------|--|
| | 12.3(4)T | This command was introduced. |
| | 12.4(24)T | Command output was updated to display address pools and prefix pools. |
| | Cisco IOS XE Release 2.1 | This command was integrated into Cisco IOS XE Release 2.1. |
| | 12.2(33)SRE | This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE. |
| | 12.2(33)XNE | This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE. |

Usage Guidelines Use the **ipv6 dhcp pool** command to create a configuration pool, and use the **ipv6 dhcp server** command to associate the configuration pool with a server on an interface.

The **show ipv6 dhcp pool** command displays DHCP for IPv6 configuration pool information. If the *poolname* argument is specified, only information on the specified pool is displayed. If the *poolname* argument is not specified, information about all pools is shown.

Examples The following sample output displays DHCP for IPv6 configuration pool information:

```
Router# show ipv6 dhcp pool

DHCPv6 pool: svr-p1
Static bindings:
  Binding for client 000300010002FCA5C01C
    IA PD: IA ID 00040002,
      Prefix: 3FFE:C00:C18:3::/72
      preferred lifetime 604800, valid lifetime 2592000
    IA PD: IA ID not specified; being used by 00040001
      Prefix: 3FFE:C00:C18:1::/72
      preferred lifetime 240, valid lifetime 54321
      Prefix: 3FFE:C00:C18:2::/72
      preferred lifetime 300, valid lifetime 54333
      Prefix: 3FFE:C00:C18:3::/72
      preferred lifetime 280, valid lifetime 51111
```

■ **show ipv6 dhcp pool**

```

Prefix from pool: local-p1, Valid lifetime 12345, Preferred lifetime 180
DNS server: 1001::1
DNS server: 1001::2
Domain name: example1.net
Domain name: example2.net
Domain name: example3.net
Active clients: 2

```

Table 115 describes the significant fields shown in the display.

Table 115 *show ipv6 dhcp pool Field Descriptions*

| Field | Description |
|------------------------------------|--|
| DHCPv6 pool: svr-p1 | The name of the pool. |
| IA PD | Identity association for prefix delegation (IAPD), which is a collection of prefixes assigned to a client. |
| IA ID | Identifier for this IAPD. |
| Prefix | Prefixes to be delegated to the indicated IAPD on the specified client. |
| preferred lifetime, valid lifetime | Lifetimes, in seconds, associated with the prefix statically assigned to the specified client. |
| DNS server | IPv6 addresses of the DNS servers. |
| Domain name | Displays the DNS domain search list. |
| Active clients | Total number of active clients. |

Related Commands

| Command | Description |
|-------------------------|---|
| ipv6 dhcp pool | Configures a DHCP for IPv6 configuration information pool and enters DHCP for IPv6 pool configuration mode. |
| ipv6 dhcp server | Enables DHCP for IPv6 service on an interface. |

show ipv6 dhcp relay binding

To display relay bindings from the Dynamic Host Configuration Protocol (DHCP) for IPv6 server binding table, use the **show ipv6 dhcp relay binding** command in user EXEC or privileged EXEC mode.

```
show ipv6 dhcp relay binding [vrf vrf-name]
```

| | |
|---------------------------|--|
| Syntax Description | vrf vrf-name (Optional) Specifies a virtual routing and forwarding (VRF) configuration. |
|---------------------------|--|

| | |
|----------------------|-------------------------------------|
| Command Modes | User EXEC (> Privileged EXEC (#) |
|----------------------|-------------------------------------|

| Command History | Release | Modification |
|------------------------|---------------------------|---|
| | 15.1(2)S | This command was introduced. |
| | Cisco IOS XE Release 3.3S | This command was integrated into Cisco IOS XE Release 3.3S. |

| | |
|-------------------------|--|
| Usage Guidelines | If the vrf vrf-name keyword and argument combination is specified, all bindings belonging to the specified VRF are displayed. |
|-------------------------|--|

| | |
|-----------------|---|
| Examples | The following sample allows you to display DHCP for IPv6 relay binding information: |
|-----------------|---|

```
Router# show ipv6 dhcp relay binding
```

show ipv6 eigrp events

To display Enhanced Interior Gateway Routing Protocol (EIGRP) events logged for IPv6, use the **show ipv6 eigrp events** command in user EXEC or privileged EXEC mode.

```
show ipv6 eigrp events [[errmsg | sia] [event-num-start event-num-end] | type]
```

| Syntax Description | |
|------------------------|---|
| errmsg | (Optional) Displays error messages being logged. |
| sia | (Optional) Displays Stuck In Active (SIA) messages. |
| <i>event-num-start</i> | (Optional) Starting number of the event range. The range is from 1 to 4294967295. |
| <i>event-num-end</i> | (Optional) Ending number of the event range. The range is from 1 to 4294967295. |
| type | (Optional) Displays event types being logged. |

Command Default If no event range is specified, information for all IPv6 EIGRP events is displayed.

Command Modes User EXEC (>)
Privileged EXEC (#)

| Command History | Release | Modification |
|-----------------|----------|---|
| | 15.0(1)M | This command was introduced in a release earlier than Cisco IOS Release 15.0(1) on the Cisco 3845 series routers. |

Usage Guidelines The **show ipv6 eigrp events** command is used to analyze a network failure by the Cisco support team and is not intended for general use. This command provides internal state information about EIGRP and how it processes route notifications and changes.

Examples The following is sample output from the **show ipv6 eigrp events** command. The fields are self-explanatory.

```
Router# show ipv6 eigrp events

Event information for AS 65535:
1 00:56:41.719 State change: Successor Origin Local origin
2 00:56:41.719 Metric set: 2555:5555::/32 4294967295
3 00:56:41.719 Poison squashed: 2555:5555::/32 lost if
4 00:56:41.719 Poison squashed: 2555:5555::/32 rt gone
5 00:56:41.719 Route installing: 2555:5555::/32 FE80::ABCD:4:EF00:1
6 00:56:41.719 RDB delete: 2555:5555::/32 FE80::ABCD:4:EF00:2
7 00:56:41.719 Send reply: 2555:5555::/32 FE80::ABCD:4:EF00:1
8 00:56:41.719 Find FS: 2555:5555::/32 4294967295
9 00:56:41.719 Free reply status: 2555:5555::/32
10 00:56:41.719 Clr handle num/bits: 0 0x0
11 00:56:41.719 Clr handle dest/cnt: 2555:5555::/32 0
```

```

12 00:56:41.719 Rcv reply met/succ met: 4294967295 4294967295
13 00:56:41.719 Rcv reply dest/nh: 2555:5555::/32 FE80::ABCD:4:EF00:2
14 00:56:41.687 Send reply: 2555:5555::/32 FE80::ABCD:4:EF00:2
15 00:56:41.687 Rcv query met/succ met: 4294967295 4294967295
16 00:56:41.687 Rcv query dest/nh: 2555:5555::/32 FE80::ABCD:4:EF00:2
17 00:56:41.687 State change: Local origin Successor Origin
18 00:56:41.687 Metric set: 2555:5555::/32 4294967295
19 00:56:41.687 Active net/peers: 2555:5555::/32 65536
20 00:56:41.687 FC not sat Dmin/met: 4294967295 2588160
21 00:56:41.687 Find FS: 2555:5555::/32 2588160
22 00:56:41.687 Rcv query met/succ met: 4294967295 4294967295
23 00:56:41.687 Rcv query dest/nh: 2555:5555::/32 FE80::ABCD:4:EF00:1
24 00:56:41.659 Change queue emptied, entries: 1
25 00:56:41.659 Metric set: 2555:5555::/32 2588160

```

Related Commands

| Command | Description |
|-------------------------|---|
| clear ipv6 eigrp | Deletes entries from EIGRP for IPv6 routing tables. |
| debug ipv6 eigrp | Displays information about EIGRP for IPv6 protocol. |
| ipv6 eigrp | Enables EIGRP for IPv6 on a specified interface. |

show ipv6 eigrp interfaces

To display information about interfaces configured for Enhanced Internal Gateway Routing Protocol (EIGRP) for IPv6, use the **show ipv6 eigrp interfaces** command in user EXEC or privileged EXEC mode.

show ipv6 eigrp [*as-number*] **interfaces** [*type number*] [**detail**]

Syntax Description

| | |
|------------------|---|
| <i>as-number</i> | (Optional) Autonomous system number. |
| <i>type</i> | (Optional) Interface type. |
| <i>number</i> | (Optional) Interface number. |
| detail | (Optional) Displays detailed interface information. |

Command Modes

User EXEC
Privileged EXEC

Command History

| Release | Modification |
|--------------------------|---|
| 12.4(6)T | This command was introduced. |
| 12.2(33)SRB | This command was integrated into Cisco IOS Release 12.2(33)SRB. |
| 12.2(33)SXH | This command was integrated into Cisco IOS Release 12.2(33)SXH. |
| Cisco IOS XE Release 2.1 | This command was introduced on Cisco ASR 1000 Series Routers. |

Usage Guidelines

Use the **show ipv6 eigrp interfaces** command to determine on which interfaces EIGRP is active, and to learn information about EIGRP relating to those interfaces. If an interface is specified, only that interface is displayed. Otherwise, all interfaces on which EIGRP is running are displayed.

If an autonomous system is specified, only the routing process for the specified autonomous system is displayed. Otherwise, all EIGRP processes are displayed.

Examples

The following is sample output from the **show ipv6 eigrp interfaces** command:

```
Router# show ipv6 eigrp 1 interfaces

IPv6-EIGRP interfaces for process 1

Interface      Peers    Xmit Queue   Mean    Pacing Time   Multicast    Pending
              0        Un/Reliable  SRTT    Un/Reliable   Flow Timer   Routes
Et0/0          0         0/0          0       0/10          0            0
```

The following is sample output from the **show ipv6 eigrp interfaces** command using the **detail** keyword:

```
Router# show ipv6 eigrp interfaces detail

IPv6-EIGRP interfaces for process 1

              Xmit Queue   Mean    Pacing Time   Multicast    Pending
```

```

Interface      Peers  Un/Reliable  SRTT    Un/Reliable  Flow Timer  Routes
Et0/0         0      0/0          0       0/10         0           0
Hello interval is 5 sec
Next xmit serial <none>
Un/reliable mcasts: 0/0 Un/reliable ucasts: 0/0
Mcast exceptions: 0 CR packets: 0 ACKs suppressed: 0
Retransmissions sent: 0 Out-of-sequence rcvd: 0
Authentication mode is not set

```

Table 116 describes the significant fields shown in the display.

Table 116 *show ipv6 eigrp interfaces Field Descriptions*

| Field | Description |
|-------------------------|---|
| Interface | Interface over which EIGRP is configured. |
| Peers | Number of directly connected EIGRP neighbors. |
| Xmit Queue Un/Reliable | Number of packets remaining in the Unreliable and Reliable transmit queues. |
| Mean SRTT | Mean smooth round-trip time (SRTT) interval (in seconds). |
| Pacing Time Un/Reliable | Pacing time (in seconds) used to determine when EIGRP packets should be sent out the interface (unreliable and reliable packets). |
| Multicast Flow Timer | Maximum number of seconds in which the router will send multicast EIGRP packets. |
| Pending Routes | Number of routes in the packets in the transmit queue waiting to be sent. |
| Hello interval is 5 sec | Length (in seconds) of the hello interval. |

show ipv6 eigrp neighbors

To display the neighbors discovered by Enhanced Interior Gateway Routing Protocol (EIGRP) for IPv6, use the **show ipv6 eigrp neighbors** command in user EXEC or privileged EXEC mode.

show ipv6 eigrp neighbors [*interface-type* | *as-number* | **static** | **detail**]

| Syntax Description | |
|-----------------------|--|
| <i>interface-type</i> | (Optional) Interface type. |
| <i>as-number</i> | (Optional) Autonomous system number. |
| static | (Optional) Displays static routes. |
| detail | (Optional) Displays detailed neighbor information. |

| Command Modes | |
|---------------|-----------------|
| | User EXEC |
| | Privileged EXEC |

| Command History | Release | Modification |
|-----------------|--------------------------|---|
| | 12.4(6)T | This command was introduced. |
| | 12.2(33)SRB | This command was integrated into Cisco IOS Release 12.2(33)SRB. |
| | 12.2(33)SXH | This command was integrated into Cisco IOS Release 12.2(33)SXH. |
| | Cisco IOS XE Release 2.1 | This command was introduced on Cisco ASR 1000 Series Routers. |

Usage Guidelines Use the **show ipv6 eigrp neighbors** command to determine when neighbors become active and inactive. It is also useful for debugging certain types of transport problems.

Examples The following is sample output from the **show ipv6 eigrp neighbors** command:

```
Router# show ipv6 eigrp neighbors
```

```
IPv6-EIGRP neighbors for process 1
```

```
H Address                Interface      Hold      Uptime     SRTT      RTO      Q      Seq
                    (sec)         00:00:13  11       200      0      2
0 Link-local address:    Et0/0         14
FE80::A8BB:CCFF:FE00:200
```

[Table 116](#) describes the significant fields shown in the display.

Table 117 *show ipv6 eigrp neighbors Field Descriptions*

| Field | Description |
|-------------------------------------|---------------------------------|
| process 1 | Autonomous system number. |
| Address FE80::A8BB:CCFF:FE00:200 | IPv6 address of the EIGRP peer. |

Table 117 *show ipv6 eigrp neighbors Field Descriptions (continued)*

| Field | Description |
|-----------|--|
| Interface | Interface on which the router is receiving hello packets from the peer. |
| Hold | Length of time (in seconds) that the Cisco IOS software will wait to hear from the peer before declaring it down. If the peer is using the default hold time, this number will be less than 15. If the peer configures a nondefault hold time, the nondefault hold time will be displayed. |
| Uptime | Elapsed time (in hours:minutes:seconds) since the local router first heard from this neighbor. |
| SRTT (ms) | Smoothed round-trip time (SRTT). The number of milliseconds required for an EIGRP packet to be sent to this neighbor and for the local router to receive an acknowledgment of that packet. |
| RTO | Retransmission timeout (in milliseconds). This is the amount of time the software waits before resending a packet from the retransmission queue to a neighbor. |
| Q count | Number of EIGRP packets (update, query, and reply) that the software is waiting to send. |
| Seq Num | Sequence number of the last update, query, or reply packet that was received from this neighbor. |

The following is sample output from the **show ipv6 eigrp neighbors** command with the **detail** keyword:

```
Router# show ipv6 eigrp neighbors detail
```

```
IPv6-EIGRP neighbors for process 1
H Address Interface Hold Uptime SRTT RTO Q Seq
(sec) (ms) Cnt Num
0 Link-local address: Et0/0 11 00:00:30 11 200 0 2
FE80::A8BB:CCFF:FE00:200
Version 12.4/1.2, Retrans: 0, Retries: 0
```

[Table 118](#) describes the significant fields shown in the display.

Table 118 *show ipv6 eigrp neighbors detail Field Descriptions*

| Field | Description |
|---------|---|
| H | This column lists the order in which a peering session was established with the specified neighbor. The order is specified with sequential numbering starting with 0. |
| Version | The software version that the specified peer is running. |
| Retrans | The number of times that a packet has been retransmitted. |
| Retries | The number of times an attempt was made to retransmit a packet. |

The following is sample output from the **show ipv6 eigrp neighbors** command with the **static** keyword:

```
Router# show ipv6 eigrp neighbors static
```

```
IPv6-EIGRP neighbors for process 1
Static Address Interface
```

■ **show ipv6 eigrp neighbors**

```
Link-local address: Ethernet0/0  
FE80::A8BB:CCFF:FE00:200
```