IP Multiplexing

You can use IP multiplexing to optimize IPv4 and IPv6 traffic in environments, such as a satellite network, where packet-per-second transmission limitations cause inefficient bandwidth utilization. IP multiplexing addresses this constraint by bundling smaller packets into one larger UDP packet, known as a superframe. The device then sends the superframe to the destination device, which demultiplexes the individual packets out of the superframe and routes them to their final destination.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to https://cfnng.cisco.com/. An account on Cisco.com is not required.

Feature Information for IP Multiplexing

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1: Feature Information for IP Multiplexing

Feature Name	Releases	Feature Information
IP Multiplexing	Cisco IOS XE Amsterdam 17.2	This features introduces IP multiplexing support on Cisco 4000 Series ISRs to optimize IPv4 and IPv6 traffic in environments such as a satellite network, where packet-per-second transmission limitations causes inefficient bandwidth utilization.

Prerequisites for IP Multiplexing

You must configure an access list before IP multiplexing can work. Create an access control list (ACL) list by using the **ip access-list** or the **ipv6 access-list** command. When you configure an ACL to use with IP multiplexing, filter only traffic based on the destination address, destination port, and protocol type. If you configure an ACL with other filter characteristics, unexpected or undesirable multiplexing decisions might occur.

Requirements and Limitations for IP Multiplexing

- IP multiplexing ACL does not support TCP traffic. You can use WAAS or WAASe to send the TCP traffic over your network.
- IP multiplexing ACL does not support call signaling traffic. The packet size of the call signaling traffic varies and UDP-based signaling can cause packet reordering.
- When you make changes to the access list, ensure that you shutdown the IP multiplexing profile.
- Ensure that you configure IP multiplexing on both ends of the link before configuring the **no shutdown** command. Otherwise, it creates a blackhole traffic until you configure the far-end.
- Ensure that the Source IP address or the Source Interface of the router matches the destination address of the other router. IP multiplexing performs source address verification and accepts packet only from known destinations.
- For VoIP device , holdtime should match packetization rate. The default packetization rate on Cisco VoIP device is 20 ms. When you set the holdtime to 20 ms, it ensures that the superframe contains only one packet from a given VoIP stream.
- Currently, IP multiplexing feature is supported only on Cisco 4000 Series ISRs.
- If you have the small and large packets in the same flow, the device can crash.
- IP multiplexing feature is tested on the following WAN interfaces: GigabitEthernet, GigabitEthernet sub interface, and GRE(IPv4/IPv6). It may have risks in other types of interfaces.
- IPsec is not supported.

- When you enable IP multiplexing debug commands with high IP multiplexing traffics, the router may crash. It is not recommended to enable IP multiplexing debug commands.

Information About IP Multiplexing

About IP Multiplexing

You can use IP multiplexing to optimize IPv4 and IPv6 traffic in environments, such as a satellite network, where packet-per-second transmission limitations cause inefficient bandwidth utilization. IP multiplexing addresses this constraint by bundling smaller packets into one larger UDP packet, known as a superframe. The device then sends the superframe to the destination device, which demultiplexes the individual packets out of the superframe and routes them to their final destination.

Traffic Identification with Access Control Lists

IP multiplexing uses Cisco access control lists (ACLs) to identify outbound packets. IP multiplexing uses ACL definitions to identify traffic selected for multiplexing treatment. You can configure standard, extended, or named ACLs to define traffic you want to multiplex. Packets that are not identified by an ACL used for multiplexing are routed normally.

In general, an ACL statement for IP multiplexing should have this format:

permit udp any *host destination-IP-address UDP-port-number*

IP multiplexing makes caching decisions based on destination IP address, destination port, and protocol type. Although ACLs can be defined to filter packets based on other attributes, using other attributes in an IP multiplexing ACL can have unexpected and unwanted results.

IP multiplexing maintains the cache of recent ACL lookup results to optimize traffic classification.

For information about configuring an ACL, see the *Security Configuration Guide: Access Control Lists* publication.

Interface Types Supported with IP Multiplexing

These interface types support IP multiplexing:

- Ethernet
- Fast Ethernet
- Gigabit Ethernet
- Gigabit Ethernet subinterface
- GRE(IPv4/IPv6)
- IPv4 generic routing encapsulation (GRE) tunnel
- IPv6 GRE tunnel
- Ethernet, Fast Ethernet, and Gigabit Ethernet VLAN

- IPsec is not supported in GRE tunnel.

Both endpoints of the multiplex connection must be configured for multiplexing with corresponding source and destination addresses. If a superframe arrives at an interface with IP multiplexing not configured or not configured to receive superframes from the destination device, the superframe is not demultiplexed, and the superframe is routed normally. If IP multiplexing is not configured, then outbound packets are routed normally.

IP Multiplexing Profiles

The attributes associated with an IP multiplexing connection between two devices are configured in an IP multiplexing profile.

Note You must configure an IP multiplexing profile for each endpoint of an IP multiplexing connection in the network.

You must define the following information for an IP multiplexing profile:

- Profile name
- ACL used to classify outbound IP packets as IP multiplexing traffic
- Source and destination IP addresses to be included in the superframe header
- Maximum amount of time the device waits to fill a superframe before sending a partial superframe

You can define the following optional information for an IP multiplexing profile:

- Maximum size of an outbound IP packet to be considered for multiplexing
- Maximum MTU size of a superframe
- Time-to-live (TTL) value to be included in the superframe IP header

IP Multiplexing Policies

An IP multiplexing policy is used to retain differentiated services code point (DSCP) priorities of the underlying data traffic. If you configure an IP multiplexing policy, you can configure DSCP values for the superframe header and specify that only the packets with a specified DSCP value be placed into the superframe. Note that a policy can match more than one DSCP value.

A device can have up to three multiplex policies for IPv6 and three multiplex policies for IPv4 defined on it. Multiplexing policies are global and apply to all multiplexing profiles on a device.

If the DSCP value assigned to a packet does not match any multiplexing policy, the device uses the default multiplexing policy for superframe multiplexing. Superframes for the default policy have a DSCP value set to 0.

If you do not configure an IP multiplexing policy, all IP multiplexing packets are sent using the default IP multiplexing policy with a DSCP value equal to 0.

The DSCP values in each packet header remains intact as the packet goes through the multiplexing and demultiplexing processes.

How to Configure IP Multiplexing

Configuration Limitation for IP Multiplexing

- When you execute the **ipmux profile showdown** command, you can have limitation with netconf configuration. You must separately commit the **ipmux profile showdown** command.

```
PE2_RP_0(config)# ip mux profile profile-1
PE2_RP_0(config-ipmux-prof)# shutdown
PE2_RP_0(config-ipmux-prof)# show configuration
ip mux profile profile-1
shutdown
!
PE2_RP_0(config-ipmux-prof)# commit
Commit complete.
PE2_RP_0(config-ipmux-prof)#
```

  Remove the IP multiplexing configuration from the interface if all profiles are shutdown. Otherwise, it might impact the normal routing performance.
- Configure the **epbr punt-policer** command if the IP multiplexing traffic drops with high scaling and throughput. For a hub router, configure the default value as: **platform punt-policer epbr 3800**. For a spoke router, configure the default value as: **platform punt-policer epbr 1000**.

```
Devive#sh platform hardware qfp active infrastructure punt statistics type per-cause |
 i epbr
143 epbr packets 1616749 1616749
```

```
PE2#sh platform hardware qfp active infrastructure punt config cause 143
QFP Punt Table Configuration

Punt table base addr : 0x30677410
punt cause index 143
punt cause name epbr packets
maximum instances 1
punt table address : 0x3067764C
instance[0] ptr : 0x30677E5C
QFP interface handle : 2
Interface name : internal0/0/rp:0
instance address : 0x30677E5C
fast failover address : 0x30658C74
Low priority policer : 158
High priority policer : 159
```

```
Devie#show platform hardware qfp active infrastructure punt policer | se 158
158 3800 0 3800 0 0 Off
020 130158 0
158 0 0
```

- To implement the IP multiplexing feature, there are two paths for IP multiplexing traffic transmission: Fast and Slow paths. The fast path includes only LAN interfaces such as Ethernet, tunnel, HDLC, and FrameRelay. Other interfaces are included in the slow path. For the slow path, you must configure the SPD with minimum threshold that is larger than 300 ms. Otherwise, it drops packets with high scaling and throughput.

```
Device(config)#ip spd queue max-threshold 301
PE2(config)#ip spd queue min-threshold 300
```

```
Devie(config)#ipv6 spd queue max-threshold 301
PE2(config)#ipv6 spd queue min-threshold 300
```

It drops packets while executing the show running, routing protocol or unused interface flapping under scaling.

- The IP multiplexing feature scaling and performance numbers are:

```
Hub router(ISR4451):
50 IPMUX profiles;
5K routes;
5K pps bidirectional IPMUX traffics;
Background traffics should be less than IPMUX;

Spoke router(ISR4321):
10 IPMUX profiles;
500 routes;
1K pps bidirectional IPMUX traffics;
Background traffics should be less than IPMUX;
```

- Configure the **deny any any** command when you configure the IPv6 access control list for IP multiplexing.

```
ipv6 access-list profile-ipv6-acl
permit udp any host 2000::1
deny any any
```

- The default IP multiplexing MTU value is 1500 bytes. The default MTU value is set when IP Multiplexing does not discover the MTU path in order to set the MTU command. This command must be manually configured by the customer which should be similar to the MTU of their network. GRE or other tunneling mechanisms reduces the overall link MTU. The MTU of IP multiplexing should be set at or lower than the link MTU value.

```
Device (config-ipmux-profile-v6)#mtu ?
<256-1500> Maximum superframe length

Device #show ip mux profile
Profile profile-ipv4
Shutdown: No
Destination: 101.0.1.2
Source: 101.0.1.1 (GigabitEthernet1/0/1)
Access-list: profile-ipv4-acl
TTL: 64
Max mux length: 1472
MTU: 1500
Hold time(ms): 21
Single packet superframes: Enabled

Device #show ipv6 mux profile
Profile profile-ipv6
Shutdown: No
Destination: 2001::1:0:2
Source: 2001::1:0:1 (GigabitEthernet1/0/1)
Access-list: profile-ipv6-acl
TTL: 64
Max mux length: 1452
MTU: 1500
Hold time(ms): 21
Single packet superframes: Enabled
```

Configuring an IP Multiplexing Profile

You must configure an IP multiplexing profile for each endpoint of an IP multiplexing connection in the network.

When configuring IP multiplexing, you must configure each device before enabling the configuration. Failure to do so will result in lost packets at the end that is not yet configured.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Enter one of the following commands:
   - **ip mux profile** *profile-name*
   - **ipv6 mux profile** *profile-name*
4. **access-list** {*standard-access-list-number* | *extended-access-list-number* | *name*}
5. **source** {*ip-addr* | *ipv6-addr* | **interface** *type*}
6. **destination** {*ip-addr* | *ipv6-addr*}
7. **holdtime** *milliseconds*
8. **maxlength** *bytes*
9. **mtu** *bytes*
10. **ttl** *hops*
11. **no singlepacket**
12. **no shutdown**
13. **end**
14. Enter one of the following commands:
    - **show ip mux profile** [*profile-name*]
    - **show ipv6 mux profile** [*profile-name*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	Enter one of the following commands: • **ip mux profile** *profile-name* • **ipv6 mux profile** *profile-name* **Example:** `Device(config)# ip mux profile routeRTP-SJ`	Creates an IP multiplexing profile with the specified name and enters IP multiplexing profile configuration mode.
Step 4	**access-list** {*standard-access-list-number* | *extended-access-list-number* | *name*} **Example:** `Device(config-ipmux-profile)# access-list routeRTP-SJ`	Applies the specified access list to the profile and uses the statements in the access list to identify outbound traffic for multiplexing. • *standard-access-list-number*—The range is 1 to 199.

	Command or Action	Purpose
		• *extended-access-list-number*—The range is 1300 to 2699. • *name*—Access list name to use with the IP multiplexing profile.
Step 5	**source** {*ip-addr* | *ipv6-addr* | **interface** *type*} **Example:** `Device(config-ipmux-profile)# source 192.0.2.1`	Designates the source IP address for the profile. • The source address is the IP address assigned to the outbound interface. • If you created an IPv4 profile, use an IPv4 address. If you created an IPv6 profile, use an IPv6 address. • If you use the **interface** keyword, IP multiplexing uses the IP address configured for that interface. Beware if you are using the **interface** keyword for an IPv6 interface with multiple IP addresses assigned to it. IP multiplexing might not use the IP address you want for multiplexing. • You must shut down the profile to change the source address. **Note** This source address must be configured as the destination address in the corresponding profile at the other end of the IP multiplexing connection.
Step 6	**destination** {*ip-addr* | *ipv6-addr*} **Example:** `Device(config-ipmux-profile)# destination 198.51.100.1`	Designates the IP address to which superframes will be sent from the particular profile. • The destination address must match the source address of the corresponding profile on the destination device. • If you created an IPv4 profile, use an IPv4 address. If you created an IPv6 profile, use an IPv6 address. • You must shut down the profile to change the destination address. **Note** This destination address must be configured as the source address in the corresponding profile at the other end of the IP multiplexing connection.
Step 7	**holdtime** *milliseconds* **Example:** `Device(config-ipmux-profile)# holdtime 150`	(Optional) Configures the amount of time in milliseconds (ms) that a multiplexing profile waits to fill the superframe before sending a partial superframe. • The range is 20 to 250 ms.

	Command or Action	Purpose
		• If you do not set a hold time, the profile uses 20 ms as a default.
Step 8	**maxlength** *bytes* **Example:** `Device(config-ipmux-profile)# maxlength 128`	(Optional) Configures the largest packet size that the multiplexing profile can hold for multiplexing. • A larger packet size will not be multiplexed even if it correctly matches the ACL attached to the profile. • The range is 64 to 1472 bytes. • If you do not configure a maximum packet length, any packet that fits into the superframe is multiplexed.
Step 9	**mtu** *bytes* **Example:** `Device(config-ipmux-profile)# mtu 1400`	(Optional) Configures the maximum size, in bytes, for the outbound superframe. • The range is 256 to 1500. • If you do not configure a MTU values, the profile uses 1500 bytes as a default. • The superframe size specified in the **mtu** command includes the IP and UDP headers for the superframe of 48 bytes for IPv6 and 28 bytes for IPv4 packets. Therefore an IPv6 MTU configured to 1400 bytes will accept 1352 bytes of data before sending a full superframe. An IPv4 MTU configured to 1400 bytes will accept 1372 bytes of data before sending a full superframe.
Step 10	**ttl** *hops* **Example:** `Device(config-ipmux-profile)# ttl 128`	(Optional) Configures the superframe time-to-live (TTL) for the IP header of the superframe. • The range is 1 to 255 hops. • By default, the TTL value is set to 64 hops.
Step 11	**no singlepacket** **Example:** `Device(config-ipmux-profile)# no singlepacket`	Configures the device to send the original packet unmodified if there is only one packet to multiplex when the hold timer expires. • By default, single packets are multiplexed into superframes when the hold timer expires.
Step 12	**no shutdown** **Example:** `Device(config-ipmux-profile)# no shutdown`	Activates the multiplexing profile. • If you want to change the ACL associated with the profile or the contents of the ACL, you must enter the **shutdown** command for the profile, make the changes and then enter the **no shutdown** command.

	Command or Action	Purpose
Step 13	**end** **Example:** `Device(config-ipmux-profile)# end`	Returns to privileged EXEC mode.
Step 14	Enter one of the following commands: • **show ip mux profile** [*profile-name*] • **show ipv6 mux profile** [*profile-name*] **Example:** `Device# show ip mux profile routeRTP-SJ`	Displays IP multiplexing statistics.

Configuring IP Multiplexing on an Interface

You must configure an interface for IP multiplexing. Once IP multiplexing is configured on an interface, all multiplex profiles are used to classify IP packets routed for transmission on the interface.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. Enter one of the following commands:
   - **ip mux**
   - **ipv6 mux**
5. **end**
6. **show interface**
7. **show** {**ip** | **ipv6**} **mux interface**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Device(config)# interface fastethernet 0/1`	Enters interface configuration mode for the specified interface.

	Command or Action	Purpose
Step 4	Enter one of the following commands: • **ip mux** • **ipv6 mux** **Example:** `Device(config-if)# ipv6 mux`	Enables IP multiplexing on the interface. • Use the **ip mux** command for an IPv4 interface. • Use the **ipv6 mux** command for an IPv6 interface.
Step 5	**end** **Example:** `Device(config-if)# end`	Returns to privileged EXEC mode.
Step 6	**show interface** **Example:** `Device# show interface`	Verifies that the interface is administratively up and whether the interface has an IPv4 or IPv6 address configured.
Step 7	**show** {**ip** | **ipv6**} **mux interface** **Example:** `Device# show ipv6 mux interface`	Displays IPv4 or IPv6 multiplexing statistics for the interface (depending on the command entered).

Configuring the UDP Port for Superframe Traffic

IP multiplexing addresses this constraint by bundling smaller packets into one larger UDP packet, known as a superframe. The device then sends the superframe to the destination device, which demultiplexes the individual packets out of the superframe and routes them to their final destination.

The receiving device identifies incoming superframes by destination IP address, protocol type (UDP), and a UDP port number. A single UDP port number is used for all IP multiplexing traffic in the network.

Note If you do not configure a UDP port for IP multiplexing traffic, the system uses the default value of 6682. This value is inserted in the UDP header of the outbound superframe. If you use the default UDP port value, make sure that all devices sending or receiving IP multiplexing traffic use the same value.

This procedure is optional and can be used to optimize IP multiplexing.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Enter one of the following commands:
   - **ip mux udpport** *port-number*
   - **ipv6 mux udpport** *port-number*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	Enter one of the following commands: • **ip mux udpport** *port-number* • **ipv6 mux udpport** *port-number* **Example:** `Device(config)# ip mux udpport 5000`	Specifies a destination UDP port to use for multiplexed packets. • The range is 1024 to 49151.

Configuring the IP Multiplexing Lookup Cache Size

The lookup cache maps the destination address, protocol type, and port number to a multiplexing profile to reduce performance overhead related to ACL lookups. You can configure the maximum size of the cache to manage memory utilization on the device.

The size of the IPv6 cache is 1,000,000 to 4,294,967,295 bytes, which corresponds to 10,419 to 44,739,242 entries.

The size of the IPv4 cache is 1,000,000 to 4,294,967,295 bytes which corresponds to 11,363 to 49,367,440 entries.

Note If you do not configure the cache size, the cache size defaults to 1,000,000 bytes, which will hold 11,363 entries for IPv4 multiplexing and 10,419 for IPv6 multiplexing.

This procedure is optional and can be used to optimize IP multiplexing.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip mux cache** *size*
4. **end**
5. **show** {**ip** | **ipv6**} **mux cache**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Device> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ip mux cache** *size* **Example:** `Device(config)# ip mux cache 5000000`	Configures the size of the IP multiplexing lookup cache. • The range is 1,000,000 to 4,294,967,295 bytes.
Step 4	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.
Step 5	**show** {**ip** | **ipv6**} **mux cache** **Example:** `Device# show ip mux cache`	Displays IPv4 or IPv6 multiplexing cache statistics (depending on the command entered).

Configuring the IP Multiplexing Policy with a DSCP Value for Outbound Superframes

Perform this task to create a multiplexing policy, specify the matching DSCP values for a superframe, and specify the outbound DSCP value for the header of the superframe.

If you do not configure a DSCP value for an outbound superframe, superframes are sent with a DSCP equal to 0.

If the DSCP value for packets selected for multiplexing does not match any of the **matchdscp** command values in the multiplexing policy, these packets are sent using the default multiplexing policy that has a DSCP set to 0.

A packet found to match the **matchdscp** command value is put in the superframe with the corresponding multiplexing policy.

This procedure is optional and can be used to optimize IP multiplexing.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Enter one of the following commands:
   - **ip mux policy** *policy-name*
   - **ipv6 mux policy** *policy-name*
4. **outdscp** *DSCP-value*
5. **matchdscp** *DSCP-value*

6. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	Enter one of the following commands: • **ip mux policy** *policy-name* • **ipv6 mux policy** *policy-name* **Example:** `Device(config)# ip mux policy RouteRTP-SJ`	Configures an IP policy with the specified name and enters either IP or IPv6 multiplexing policy configuration mode (depending on the command entered).
Step 4	**outdscp** *DSCP-value* **Example:** `Device(config-ipmux-policy)# outdscp 10`	Configures the DSCP value for the outbound superframe. • The range is 0 to 63. • For additional DSCP values that are valid, see the *IP Mobility Command Reference*.
Step 5	**matchdscp** *DSCP-value* **Example:** `Device(config-ipmux-policy)# matchdscp 45`	Configures the DSCP value that IP multiplexing uses to compare against the DSCP value in packets bound for multiplexing. • A match puts the packet in the superframe that corresponds to the IP multiplex policy. • You can enter more than one value. • The range is 0 to 63. • For additional DSCP values that are valid, see the *IP Mobility Command Reference*.
Step 6	**exit** **Example:** `Device(config-ipmux-policy)# exit`	Exits IP (or IPv6) multiplexing policy configuration mode.

Configuration Examples for IP Multiplexing

Example: Configuring an IP Multiplexing Profile

The following example shows an IPv4 multiplexing profile configuration:

```
ip mux profile r1a
  destination 10.1.1.1
  source 10.1.1.2
  access-list 199
  ttl 10
  holdtime 30
  mtu 1428
  maxlength 1400
```

Example: Configuring IP Multiplexing on an Interface

The following example show an IPv4 multiplexing configuration on an interface:

```
Gigabit Ethernet 0/0
 ip mux
```

Examples: Configuring the UDP Port for Superframe Traffic

The following example shows a UDP port configuration for superframe traffic for IPv4:

```
ip mux udpport 12345
```

The following example shows a UDP port configuration for superframe traffic for IPv6:

```
ipv6 mux udpport 12345
```

Examples: Configuring the IP Multiplexing Lookup Cache Size

The following example shows an IPv4 multiplexing lookup cache size configuration:

```
ip mux cache 2000000
```

The following example shows an IPv6 multiplexing lookup cache size configuration:

```
ipv6 mux cache 2000000
```

Examples: Configuring the IP Multiplexing Policy With a DSCP Value for Outbound Superframes

The following example shows an IPv4 multiplexing policy:

```
ip mux policy dscp4
  matchdscp 4
  outdscp 4
```

The following example shows the IPv6 multiplexing policy:

```
ipv6 mux policy dscp4
  matchdscp 4
  outdscp 4
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
IP mobility commands	IP Mobility Command Reference

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html