ip mobile mobile-networks through multi-path (mobile router)

ip mobile mobile-networks

To associate one or more networks with a mobile router configured as a mobile host and enter mobile networks configuration mode, use the **ip mobile mobile-networks** command in global configuration mode. To disassociate the networks from the mobile router, use the **no** form of this command.

ip mobile mobile-networks *lower* [*upper*]

no ip mobile mobile-networks *lower* [*upper*]

Syntax Description

lower [*upper*	Range of mobile host or mobile node group IP addresses. The upper end of the range is optional but can only be used for dynamic registration of mobile networks. Static mobile network configurations are not permitted for a range of hosts.

Command Default

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.2(13)T	The *upper* argument was added to allow a range of mobile host or mobile node group addresses.

Usage Guidelines

The home agent supports mobile routers configured with the mobile networks that are roaming with the mobile routers.

The *lower* [*upper* arguments associate the mobile networks with the IP address of the mobile router, which was configured using the **ip mobile host** command. You can use the *upper* range only with dynamic mobile network registration. Static mobile network configurations are not permitted for a range of hosts.

You can configure the home agent to dynamically learn of the mobile networks during registration as shown in the following example:

```
ip mobile host 10.0.0.1 10.0.0.10 virtual-networks 10.0.0.0 255.0.0.0
ip mobile mobile-networks 10.0.0.1 10.0.0.10
!dynamic registration
 register
```

You can configure the home agent to learn of the mobile networks through static configuration as shown in the following example:

```
ip mobile host 10.0.0.1 virtual-networks 10.0.0.0 255.0.0.0
ip mobile host 10.0.0.2 virtual-networks 10.0.0.0 255.0.0.0
!
ip mobile mobile-networks 10.0.0.1
!static configuration
 network 172.16.1.0 255.255.255.0
ip mobile mobile-networks 10.0.0.2
!static configuration
 network 172.16.2.0 255.255.255.0
```

You cannot configure the range as shown in the following static configuration:

```
!static configuration not permitted for range of hosts
ip mobile mobile-networks 10.0.0.1 10.0.0.10
 network 172.16.2.0
```

The mobile router configuration is allowed only for one mobile router or an entire range of mobile routers in the mobile host group, exclusively. You cannot configure a partial range of mobile routers as shown in the following example:

```
ip mobile host 10.0.0.1 10.0.0.10 virtual-network 10.0.0.0 255.0.0.0
!Partial range shown below is prohibited
ip mobile mobile-networks 10.0.0.1 10.0.0.3
 register
```

You cannot combine full ranges and partial ranges of IP addresses in a configuration as shown in the following example:

```
ip mobile host 10.0.0.1 10.0.0.10 virtual-network 10.0.0.0 255.0.0.0
ip mobile mobile-networks 10.0.0.1 10.0.0.10
 register
ip mobile mobile-networks 10.0.0.2
 network 172.16.2.0 255.255.255.0
```

Examples

The following example configures the mobile host, which is a mobile router at 10.1.1.10, and associates it with the mobile networks that it is supporting:

```
ip mobile host 10.1.1.10 virtual-network 10.0.0.0 255.0.0.0
ip mobile mobile-networks 10.1.1.10
 network 172.6.2.0 255.255.255.0
ip mobile secure host 10.1.1.10 spi 100 key hex 12345678123456781234567812345678
```

The following example shows the mobile router configured for both static and dynamic mobile networks:

```
ip mobile host 10.1.1.10 virtual-network 10.0.0.0 255.0.0.0
ip mobile mobile-networks 10.1.1.10
 network 172.16.1.0 255.255.255.0
 register
```

Related Commands

Command	Description
ip mobile host	Associates a mobile router with mobile networks.
register (mobile router)	Dynamically registers the mobile networks with the home agent.
show ip mobile mobile-networks	Displays a list of mobile networks associated with the mobile router.

ip mobile prefix-length

To append the prefix-length extension to the advertisement, use the **ip mobile prefix-length** command in interface configuration mode. To restore the default, use the **no** form of this command.

ip mobile prefix-length

no ip mobile prefix-length

Syntax Description

This command has no arguments or keywords.

Command Default

The prefix-length extension is not appended.

Command Modes

Interface and Global configuration

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.3(11)T	Global configuration mode was added.

Usage Guidelines

The prefix-length extension is used for movement detection. When a mobile node registered with one foreign agent receives an agent advertisement from another foreign agent, the mobile node uses the prefix-length extension to determine whether the advertisements arrived on the same network. The mobile node needs to register with the second foreign agent if it is on a different network. If the second foreign agent is on the same network, reregistration is not necessary.

Examples

The following example appends the prefix-length extension to agent advertisements sent by a foreign agent:

```
ip mobile prefix-length
```

Related Commands

Command	Description
show ip mobile interface	Displays advertisement information for interfaces that are providing foreign agent service or are home links for mobile nodes.

ip mobile proxy-host

To locally configure the proxy Mobile IP attributes, use the **ip mobile proxy-host**command in global configuration mode. To remove the configuration, use the no form of this command.

ip mobile proxy-host nai *username realm* [**flags** *rrq-flags*] [**home-agent** *ip-address*] [**home-addr** *home-address*] [**lifetime** *seconds*] **[local-timezone]**

no ip mobile proxy-host nai *usernam realm* [**flags** *rrq-flags*] [**home-agent** *ip-address*] [**home-addr** *home-address*] [**lifetime** *seconds*] **[local-timezone]**

Syntax Description

nai *username@realm*	Network access identifier.
flags *rrq-flags*	(Optional) Registration request flags.
home-agent *ip-address*	(Optional) IP address of the home agent.
home-addr *home-address*	(Optional) Home IP address of the mobile node.
lifetime *seconds*	(Optional) Global registration lifetime for a mobile node. Note that this can be overridden by the individual mobile node configuration. Values are from 3 to 65535 (infinity). Default is 36000 seconds (10 hours). Registrations requesting a lifetime greater than this value will still be accepted, but will use this lifetime value.
local -timezone	(Optional) Adjusts the UTC time based on the local time zone configured and uses the adjusted time for proxy mobile IP registration.

Command Default

No security association is specified.

Command Modes

Global configuration

Command History

Release	Modification
12.2(2)XC	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T for Packet Data Serving Node (PDSN) platforms.

Usage Guidelines

This command is only available on PDSN platforms running specific PDSN code images; consult Feature Navigator for your Cisco IOS software release.

All proxy Mobile IP attributes can be retrieved from the AAA server. You can use this command to configure the attributes locally.

If only a realm is specified, the home address cannot be specified.

Examples

The following example configures the Mobile IP proxy host with an IP address of 10.3.3.1 and a lifetime value of 6000 seconds:

```
ip mobile proxy-host nai moiproxy1@cisco.com flags 40 home-agent 10.3.3.1 lifetime 6000
```

Related Commands

Command	Description
ip mobile host	Configures the mobile host or mobile node group.
ntp server	Allows the system clock to be synchronized by a time server.
ip mobile secure	Configures the mobility security associations for mobile host, mobile visitor, foreign agent, home agent, or proxy mobile host.
show ip mobile proxy	Displays information about the proxy host configuration.

ip mobile radius disconnect

To enable the home agent to process Radius Disconnect messages, use the ip mobile radius disconnect command in global configuration mode. To disable the processing of Radius Disconnect messages on the home agent, use the no form of this command.

ip mobile radius disconnect

no ip mobile radius disconnect

Syntax Description

This command has no arguments or keywords.

Command Default

Radius Disconnect messages are not processed by the home agent.

Command Modes

Global configuration

Command History

Release	Modification
12.3(7)XJ	This command was introduced.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.

Usage Guidelines

In order for packet of disconnect (POD) requests to be processed by AAA, you need to configure the aaa server radius dynamic-author global configuration command.

You must configure radius-server attribute 32 include-in-access-req for the home agent to send the fully qualified domain name (FQDN) in the access request.

Examples

The following example enables the home agent to process Radius Disconnect messages:

```
Router(config)# ip mobile radius disconnect
```

ip mobile realm

To enable inbound user sessions to be disconnected when specific session attributes are presented, use the ip mobile realm command in global configuration mode. To disable this functionality, use the no form of this command.

ip mobile realm *@xyzcom* **vrf** *vrf-name* **ha-addr** *ip-address* [**aaa-group** [**accounting** *aaa-acct-group*| **authentication** *aaa-auth-group*]] [**dns dynamic-update method word**] [**dns server** *primary dns server address secondary dns server address* **[assign] [hotline]**]

no ip mobile realm *@xyzcom* **vrf** *vrf-name* **ha-addr** *ip-address* [**aaa-group** [**accounting** *aaa-acct-group*| **authentication** *aaa-auth-group*]] [**dns dynamic-update method word**] [**dns server** *primary dns server address secondary dns server address* **[assign] [hotline]**]

Syntax Description

realm	Name of the specified realm.
vrf *vrf name*	Enables VRF support for a specific group.
ha-addr *ip-address*	IP address of the Home Agent.
aaa-group	(Optional) Denotes a AAA group.
accounting *aaa-acct-group*	(Optional) Specifies a AAA accounting group.
authentication *aaa-auth-group*	(Optional) Specifies a AAA authentication group.
dns dynamic-update method word	(Optional) Enables the DNS Update procedure for the specified realm. word is the dynamic DNS update method name.
dns server *primary dns server address secondary dns server address*	(Optional) Enables you to locally configure the DNS Server address.
assign	(Optional) Enables this feature for the specified realm.
hotline	(Optional) Enables Hotlining of the mobile hosts.

Command Default

There are no default values for this command.

Command Modes

Global configuration

Command History

Release	Modification
12.3(7)XJ.	This command was introduced.

Release	Modification
12.3(14)YX	The dns server assign, and dns dynamic-update method variables were introduced.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.

Usage Guidelines

This CLI defines the VRF for the domain “@xyz.com”. The IP address of the Home Agent corresponding to the VRF is also defined, at which the MOIP tunnel will terminate. The IP address of the Home Agent should be a routable IP address on the box. Optionally, the AAA accounting and/or authentication server groups can be defined per VRF. If a AAA accounting server group is defined, all accounting records for the users of the realm will be sent to the specified group. If a AAA authentication server group is defined, HA-CHAP is sent to the server(s) defined in the group.

Examples

The following example identifies the DNS dynamic update keyword:

```
router(config)#ip mobile realm @ispxyz1.com dns ?
dynamic-update Enable 3GPP2 IP reachability
server DNS server configuration
```

The following example identifies the hotlining and vrf keywords:

```
router(config)# ip mobile realm @ispxyz1.com ?
dns Configure DNS details
hotline Hotlining of the mobile hosts
vrf VRF for the realm
```

ip mobile registration-lifetime

To set the registration lifetime value advertised, use the **ip mobile registration-lifetime** command in interface or global configuration mode.

ip mobile registration-lifetime *seconds*

no ip mobile registration-lifetime

Syntax Description

seconds	Lifetime in seconds. Range is from 3 to 65535 (infinity).

Command Default

36000 seconds

Command Modes

Interface and global configuration

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.3(11)T	Global configuration mode was added.

Usage Guidelines

This command allows an administrator to control the advertised lifetime on the interface. The foreign agent uses this command to control duration of registration. Visitors requesting longer lifetimes will be denied.

Examples

The following example sets the registration lifetime to 10 minutes on interface Ethernet 1 and 1 hour on interface Ethernet 2:

```
interface e1
 ip mobile registration-lifetime 600
interface e2
 ip mobile registration-lifetime 3600
```

Related Commands

Command	Description
show ip mobile interface	Displays advertisement information for interfaces that are providing foreign agent service or are home links for mobile nodes.

ip mobile router

To enable the mobile router and enter mobile router configuration mode, use the **ip mobile router**commandin global configuration mode. To disable the mobile router, use the **no** form of this command.

ip mobile router

no ip mobile router

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration

Command History

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

Usage Guidelines

The mobile router is a router that operates as a mobile node. The mobile router can roam from its home network and still provide connectivity for devices on its networks. The mobile networks are locally attached to the router.

Examples

The following example enables the mobile router:

```
ip mobile router
```

Related Commands

Command	Description
show ip mobile router	Displays configuration information and monitoring statistics about the mobile router.

ip mobile router-service

To enable mobile router service on an interface, use the **ip mobile router-service** command in interface configuration mode. To disable this service, use the **no** form of this command.

ip mobile router-service {**hold-down** [**foreign-agent** *seconds*| **reassociate** *msec*]| **roam** [**priority** *value*]| **solicit** [**interval** *seconds*] [**retransmit initial** *minimum* **maximum** *seconds* **retry** *number*]}

no ip mobile router-service {**hold-down** [**foreign-agent** *seconds*| **reassociate** *msec*]| **roam** [**priority** *value*]| **solicit** [**interval** *seconds*] [**retransmit initial** *minimum* **maximum** *seconds* **retry** *number*]}

Syntax Description

hold-down	Specifies a delay period for mobile router registration.
foreign-agent *seconds*	(Optional) Time (in seconds) to wait before the mobile router registers to agents heard on an interface. The default is zero. The range is from 0 to 3600 seconds.
reassociate *msec*	(Optional) Specifies the delay (in milliseconds), after receiving a linkDown trap, that the mobile router waits for a linkUp trap. The default is 1000 msec. The range is from 0 to 5000 seconds.
roam	Enables the mobile router interface to roam.
priority *value*	(Optional) Priority value that is compared among multiple configured interfaces to select the interface in which to send the registration request. When multiple interfaces have highest priority, the highest bandwidth is the preferred choice. When multiple interfaces have the same bandwidth, the interface with the highest IP address is preferred. The range is from 0 to 255; the default is 100. Higher values equate to a higher priority.
solicit	Instructs the mobile router to send agent solicitation messages periodically.
interval *seconds*	(Optional) Interval (in seconds) to wait before the mobile router sends the next agent solicitation message after an advertisement is received on an interface. The range is from 1 to 65535 seconds; the default interval is 600 seconds (10 minutes).
retransmit initial	(Optional) Wait period before a retransmission of a registration request when no reply is received. The range is from 10 to 10000 milliseconds (10 seconds); the default is 1000 milliseconds (1 second).

minimum	(Optional) Minimum wait period (in seconds) before retransmission of a registration request when no reply is received.
maximum *seconds*	(Optional) Maximum wait period (in seconds) before retransmission of a registration request when no reply is received. Each successive retransmission timeout period is twice the previous period, as long as that is less than the maximum value.
retry *number*	(Optional) Number of times to retry sending the retransmission request. Retransmission stops after the maximum number of retries are attempted. The range is from 0 to 10; the default retry is 3. A value of 0 means no retransmission.

Command Default

hold-down foreign agent *seconds:* zero**hold-down reassociate** *msec:* 1000**priority** *value*: 100**interval** *seconds*: 600 seconds**retransmit initial** *minimum* **maximum** *seconds*: 1000 milliseconds (1 second)**retry** *number*: Three retries

Command Modes

Interface configuration

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.3(14)T	The **foreign-agent** *seconds* and **reassociate** *msec* keywords and arguments were added.

Usage Guidelines

The mobile router discovers home agents and foreign agents by receiving agent advertisements.

Note In release 12.3(14)T, the **ip mobile router-service hold-down**commandwas changed to the **ip mobile router-service hold-down foreign-agent** command. The previous version of the command is still accepted but the new command will appear in the running configuration.

When a wireless link connected to an interface is lossy, the mobile router must not immediately register with the foreign agent even when heard on a preferred interface. The **ip mobile router-service hold-down foreign-agent***seconds*command allows existing communications to continue with mobile networks while the mobile router gauges the quality of the link to the new foreign agent.

The ip mobile router-service solicit command instructs the mobile router to send agent solicitation messages periodically. Some networks only send out agent advertisements periodically or when solicited. For networks on which agents do not advertise periodically, this function must be enabled to detect agents. The mobile router always sends solicitation messages when roaming interfaces come up.

If a mobile router interface is configured for solicitations, you should set both **ip irdp maxadvertinterval***seconds* and **ip irdp holdtime***seconds* to 0 seconds on the foreign agent. These settings ensure that the foreign agent will not send out any IRDP advertisements unless solicited. If a foreign agent or home agent are sending IRDP advertisements periodically, then a solicitation will trigger the agent to send an advertisement immediately instead of at the next time interval.

The solicit timer for the **ip mobile router-service solicit** command is reset and no solicitation is sent out on the roaming interface if the mobile router receives an advertisement from a foreign agent before the solicit timer expires. For example, if the mobile router is configured to solicit every 10 seconds and the foreign agent advertises every 3 seconds, the mobile router will never solicit.

Use the **ip mobile router-service hold-down reassociate** *msec* command to specify the interval of time that the mobile router will wait, after receiving an SNMP linkDown trap, for a linkUp trap from the Wireless Mobile Interface Card (WMIC) indicating that the wireless link is available for use. This hold-down delay should be long enough for the WMIC to establish connectivity with a new AP or bridge when roaming.

Use the **show ip mobile router agent** command to display agents learned from advertisements and the mobile router's available CCoAs. Use the **show ip mobile router interface** command to display the configuration of the interfaces used for roaming.

Examples

The following example configures roaming interfaces, solicitation services, and hold-down timers on serial interface 0 and roaming interfaces and hold-down timers on Ethernet interface 0 of the mobile router.

In this example, the mobile router has two interfaces. The serial interface is connected to a serial interface of a foreign agent and the Ethernet interface is connected to an Ethernet interface of a foreign agent. The mobile router will prefer to register on the Ethernet interface if possible because it has a higher priority than the serial interface. If the mobile router does not receive any agent advertisements on the Ethernet interface, it will use the serial interface to solicit foreign agents.

If the Ethernet interface hears a new foreign agent advertisement after the mobile router has already registered using the serial interface, it will wait the duration of the hold-down timer (20 seconds) before registering with the foreign agent on the Ethernet interface. The **ip mobile router-service hold-down foreign-agent***seconds*command allows communications to continue with mobile networks while the mobile router gauges the quality of the link to the new foreign agent. The Ethernet interface is configured with a higher priority so the mobile router prefers to register with this interface.

Once it receives an agent advertisement on the Ethernet interface, it will use the Ethernet interface to register to its home agent.

```
interface s0
  ip mobile router-service roam
! s0 solicits every 5 seconds after last advertisement received on the interface
  ip mobile router-service solicit interval 5
  ip mobile router-service hold-down foreign-agent 20
interface e0
  ip mobile router-service roam priority 101
  ip mobile router-service hold-down foreign-agent 20
```

In the following example, the mobile router is configured to receive dynamic CCoA from DHCP. The mobile router will wait 2000 milliseconds for the SNMP linkUp trap from the WMIC indicating that layer 2 has reassociated. This interval of time allows the mobile router to roam and still maintain wireless connectivity.

```
interface FastEthernet0
 ip address dhcp
 ip dhcp client mobile renew count 3 interval 20
 ip mobile router-service roam
```

```
ip mobile router-service collocated
ip mobile router-service hold-down reassociate 2000
```

Related Commands

Command	Description
show ip mobile router agent	Displays information about the agents for the mobile router.
show ip mobile router interface	Displays information about the interface that the mobile router is using for roaming.

ip mobile router-service collocated

To enable static or dynamic collocated care-of address (CCoA) processing on a mobile router interface, use the **ip mobile router-service collocated**command in interface configuration mode. To disable static or dynamic CCoA processing, use the **no** form of this command.

ip mobile router-service collocated [**gateway** *ip-address*] **[ccoa-only]**

no ip mobile router-service collocated [**gateway** *ip-address*] **[ccoa-only]**

Syntax Description

gateway *ip-address*	(Optional) Next hop IP address for the mobile router to forward packets. The **gateway** *ip-address*combination is only seen while configuring an Ethernet interface.
ccoa-only	(Optional) Enables the interface to use CCoA processing only.

Command Default

No default behavior or values

Command Modes

Interface configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.3(4)T	The **ccoa-only** keyword was added. Dynamic CCoA functionality was added.

Usage Guidelines

The primary IP address of the interface is used as the CCoA. The interface must already be configured as a roaming interface using the **ip mobile router-service roam** interface configuration command for both static and dynamic CCoA processing.

The mobile router can register with the home agent using a CCoA that was acquired dynamically via the IP Control Protocol (IPCP).

The gateway IP address is the next-hop IP address for registration packets. Upon successful registration, this address will be used as the default gateway and default route.

You need not specify the **gateway** *ip-address* combination if using a serial interface. The **gateway***ip-address* combination is required on all non point-to-point interfaces such as Ethernet LANs and must be on the same logical subnet as the primary interface IP address.

You can configure the mobile router interface to register only its CCoA and ignore foreign agent advertisements by using the **ip mobile router-service collocated ccoa-only** option. Using this command on an interface already registered with a foreign agent CoA will cause the mobile router to re-register immediately with a CCoA.

Using the **no ip mobile router-service collocated ccoa-only**command on an interface already registered with a CCoA will cause the interface to deregister its CCoA and begin foreign agent discovery.

Examples

The following example enables static CCoA processing on a mobile router interface:

```
interface FastEthernet0/0
! Primary IP address is the static CCoA
 ip address 172.21.58.23 255.255.255.0
 ip mobile router-service roam
! Gateway IP address is next-hop destination
 ip mobile router-service collocated gateway 172.21.58.1
```

The following example enables dynamic CCoA processing on a mobile router interface:

```
interface Serial 3/1
 ip address negotiated
 encapsulation ppp
 ip mobile router-service roam
 ip mobile router-service collocated
```

The following example enables static CCoA-only processing. The interface will not listen to foreign agent advertisements.

```
interface Ethernet 1/0
 ip address 10.0.1.1 255.255.255.0
 ip mobile router-service roam
 ip mobile router-service collocated gateway 10.0.1.2 ccoa-only
 ip mobile router-service collocated registration retry 30
```

The following example enables dynamic CCoA-only processing. The interface will not listen to foreign agent advertisements.

```
interface Serial 1/0
 ip address negotiated
 encapsulation ppp
 ip mobile router-service roam
 ip mobile router-service collocated ccoa-only
```

Related Commands

Command	Description
ip mobile router-service collocated registration retry	Configures the time period that the mobile router waits before sending another registration request after a registration failure.
ip mobile router-service roam	Enables the mobile router to discover on which configured interface it will discover foreign agents.

ip mobile router-service collocated registration nat traversal

To enable Network Address Translation (NAT) traversal support for the mobile router, use the **ip mobile router-service collocated registration nat traversal** command in interface configuration mode. To disable NAT traversal support for the mobile router, use the **no** form of this command.

ip mobile router-service collocated registration nat traversal [**keepalive** *seconds*] **[force]**

no ip mobile router-service collocated registration nat traversal [**keepalive** *seconds*] **[force]**

Syntax Description

keepalive *seconds*	(Optional) Configures the keepalive interval, in seconds, that the mobile router will use when the home agent does not offer a specific value and just returns zero. The range is from is 0 to 65535. The default is 110. When the value zero is chosen, the keepalive timer is disabled.
force	(Optional) Allows the mobile router to force the home agent to allocate a NAT UDP tunnel without performing detection presence of NAT along the HA-MR path.

Command Default

The mobile router does not support NAT traversal.

Command Modes

Interface configuration

Command History

Release	Modification
12.4(6)XE	This command was introduced.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.

Usage Guidelines

UDP tunneling is negotiated only when the mobile router registers to the home agent in collocated care-of address (CCoA) mode.

If you configure the mobile router to force the home agent to allocate a UDP tunnel but do not configure the home agent to force UDP tunneling, the home agent will reject the forced UDP tunneling request. The decision of whether to force UDP tunneling is controlled by the home agent.

Examples

The following example shows a mobile router configured with a keepalive timer set to 56 seconds and forced to request UDP tunneling.

```
ip mobile router-service collocated registration nat traversal keepalive 56 force
```

Related Commands

Command	Description
ip mobile home-agent nat traversal	Enables NAT traversal support for Mobile IP home agents.
ip mobile foreign-agent nat traversal	Enables NAT traversal support for Mobile IP foreign agents.
show ip mobile binding	Displays the mobility binding table.
show ip mobile globals	Displays global information for mobile agents.
show ip mobile tunnel	Displays information about active tunnels.
show ip mobile visitor	Displays the table that contains the visitor list of the foreign agent.

ip mobile router-service collocated registration retry

To configure the time period that the mobile router waits before sending another registration request after a registration failure, use the **ip mobile router-service collocated registration retry**command in interface configuration mode. To disable this functionality, use the **no** form of this command.

ip mobile router-service collocated registration retry *seconds*

no ip mobile router-service collocated registration retry

Syntax Description

seconds	Retry interval (in seconds) for registration requests. The range is from 1 to 65535.

Command Default

60 seconds

Command Modes

Interface configuration.

Command History

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

Usage Guidelines

An interface configured for static collocated care-of address (CCoA) will not have foreign agent advertisements to use to trigger new registration attempts. Any foreign agent advertisements detected on that interface are ignored.

The default retry value is 60 seconds. You need to use this command only when a different retry interval is desired.

Examples

The following example shows that the mobile router will wait 30 seconds before sending another registration request after a registration failure:

```
interface FastEthernet0/0
! Primary IP address is the CCoA
 ip address 172.21.58.23 255.255.255.0
 ip mobile router-service roam
 ip mobile router-service collocated gateway 172.21.58.1
 ip mobile router-service collocated registration retry 30
```

Related Commands

Command	Description
ip mobile router-service collocated	Enables static CCoA processing on a mobile router interface.

ip mobile router-service description

To add a description for the type of roaming interface that is active on the mobile router, use the **ip mobile router-service description** command in interface configuration mode. To remove the description, use the no form of this command.

ip mobile router-service description *string*

no ip mobile router-service description *string*

Syntax Description

string	Alphanumeric character string of the description of the roaming interface.

Command Default

If this command is not issued, a description does not exist.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

If the **ip mobile router-service description** command is configured, the description of the roaming interface is sent to the home agent during registration and will display in the output of the **show ip mobile binding** command.

Examples

The following example shows the description for the type of roaming interface on the mobile router:

```
interface FastEthernet0/0
 ip mobile router-service description Wireless LAN
```

Related Commands

Command	Description
show ip mobile binding	Displays the mobility binding table on the home agent.

ip mobile router-service link-type

To enable a link-type roaming interface, use the **ip mobile router-service link-type** command in interface configuration mode. To disable the link-type roaming interface, use the **no** form of this command.

ip mobile router-service link-type *link-type*

no ip mobile router-service link-type

Syntax Description

link-type	Link-type associated with a roaming interface. The following link-types are available: 1xRTT, 4.9G, 802.11a, 802.11b, 802.11g, EDGE, EVDO, GPRS, UMTS, WORD, WiMAX

Command Default

No link-type roaming interface is configured.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.4(24)T	This command was introduced.

Usage Guidelines

Use this command to configure label-based application routing and the mobile router (MR) roaming interfaces. The link-type label on the interfaces is passed to the home agent (HA) when the interface registers. This label is used during registration on both the MR and the HA to generate dynamic route maps from mobile map templates.

Example:

```
interface ethernet 1/0
 ip mobile router-service roam
 ip mobile router-service link-type 802.11g
```

Access Control Lists

You can use one or more extended named access control lists (ACLs) on both the MR and the HA to identify the application traffic. MR and HA are used as templates at registration time to generate dynamic ACLs that are used in the dynamic route maps.

Example:

```
ip access-list extended WEB
 permit udp any any eq port 8080
```

Mobile Map Mobile Policy Templates

You can use one or more mobile map mobile policy templates on the MR and HA.

Example:

```
ip mobile mobile-map MPATH_1 10
 match access-list WEB
 set link-type 802.11g  UMTS
 set interface null0
```

You need to apply the mobile map to access interfaces. The mobile map is associated with a mobile network interface on the MR in the mobile network configuration. The mobile map configuration on the HA can specify up to three ingress interfaces.

Example:

MR:

```
ip mobile router
 mobile-network e 3/0 policy mobile-map MPATH_1
```

HA:

```
ip mobile router
 ip mobile home-agent policy mobile-map e 2/0   e 3/0   e 4/0
```

On the MR, a dynamic route map is created when each mobile-map template is configured. The dynamic route map has a long name that contains the first seven characters of the mobile map tag.

Example: A mobile map with the tag “MPATH_1” creates the following dynamic route map:

```
MIP-00/00/00-01:02:03-1-MPATH_1
```

The dynamic name contains the application that generated the MIP, a date and time stamp, and a sequence number.

On the HA, a single dynamic route map is created when the first mobile map is configured. It has the following name:

```
MIP-10/11/06-01:02:03-1-MP-HA
```

Examples

The following example shows how to enable the link-type roaming interface using the **ip mobile router-service link-type**command:

```
Router> enable
Router# configure terminal
Router(config)# interface FastEthernet0/2
Router(config-if)# ip mobile router-service link-type 802.11g
```

Related Commands

Command	Description
ip mobile router-service roam	Enables the roaming interface of the IP mobile router service.

ip mobile router-service roam

To enable the roaming interface of the IP mobile router service, use the **ip mobile router-service roam** command in interface configuration mode. To disable a roaming interface, use the **no** form of this command.

ip mobile router-service roam [**priority** *priority-level*]

no ip mobile router-service roam [**priority** *priority-level*]

Syntax Description

priority	(Optional) Sets the roaming interface priority of the router service.
priority-level	(Optional) Roaming priority level. The priority level can be 50, 100, 200, and so on.

Command Default

No priority is set for roaming interfaces.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.4(24)T	This command was introduced.

Usage Guidelines

Use this command to configure label-based application routing and the mobile router (MR) roaming interfaces. The link type label on the interfaces is passed to the home agent (HA) when the interface registers. This label is used during registration on both the MR and the HA to generate dynamic route maps from mobile map templates.

Example:

```
interface ethernet 1/0
 ip mobile router-service roam
 ip mobile router-service link-type 802.11g
```

Access Control Lists (ACL)

You can use one or more extended named ACLs on both the MR and the HA to identify the application traffic. MR- and HA-named ACLs are used as templates at registration time to generate dynamic ACLs that are used in the dynamic route maps.

Example:

```
ip access-list extended WEB
 permit udp any any eq port 8080
```

Mobile Map Mobile Policy Templates

You can use one or more mobile map mobile policy templates on the MR and HA.

Example:

```
ip mobile mobile-map MPATH_1 10
 match access-list WEB
 set link-type 802.11g  UMTS
 set interface null0
```

You need to apply the mobile map to access interfaces. The mobile map is associated with a mobile network interface on the MR in the mobile network configuration. The mobile map configuration on the HA can specify up to three ingress interfaces.

Example:

MR:

```
ip mobile router
 mobile-network e 3/0 policy mobile-map MPATH_1
```

HA:

```
ip mobile router
 ip mobile home-agent policy mobile-map e 2/0   e 3/0   e 4/0
```

On the MR, a dynamic route map is created when each mobile map template is configured. The dynamic route map has a long name that contains the first seven characters of the mobile map tag.

Example: A mobile map with the tag "MPATH_1" creates the following dynamic route map:

```
MIP-00/00/00-01:02:03-1-MPATH_1
```

The dynamic name contains the application that generated the MIP, a date and time stamp, and a sequence number.

On the HA, a single dynamic route map is created when the first mobile map is configured. It has the following name:

```
MIP-10/11/06-01:02:03-1-MP-HA
```

Examples

The following example shows how to enable a roaming interface and assign a priority for it:

```
Router> enable
Router# configure terminal
Router# interface FastEthernet0/2
Router(config-if)# ip mobile router-service roam priority 101
```

Related Commands

Command	Description
ip mobile router-service link-type	Configures the link type of the roaming interface defined for a mobile router service.

ip mobile router-service tunnel mode

To set the encapsulation mode for a mobile router interface, use the **ip mobile router-service tunnel mode**command in interface configuration mode. To restore the default encapsultion mode on an interface, use the **no** form of this command.

ip mobile router-service tunnel mode {**gre**| **ipip**}

no ip mobile router-service tunnel mode

Syntax Description

gre	Specifies that the mobile router will attempt to register with Generic Routing Encapsulation (GRE) on the interface.
ipip	Specifies that IP-in-IP encapsulation will be used on the interface.

Command Default

The default encapsulation mode for Mobile IP is IP-in-IP encapsulation.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

If the **ip mobile router-service tunnel mode gre**command is configured, the mobile router will request GRE encapsulation in the registration request only if the foreign agent (FA) advertises that it is capable of GRE encapsulation (the G bit is set in the advertisement). If the registration request is successful, packets will be tunneled using GRE.

If the **ip mobile router-service tunnel mode gre**command is enabled and collocated care-of address (CCoA) is configured, the mobile router will attempt to register with the home agent (HA) using GRE encapsulation. If the registration request is successful, packets will be tunneled using GRE.

If the mobile router receives a denied registration reply with error code 72 (foreign agent required encapsulation unavailable) or error code 139 (home agent unsupported encapsulation), the mobile router will send another registration request with the G bit unset and IP-in-IP encapsulation will be used.

The **no ip mobile router-service tunnel mode**command instructs the mobile router to revert to the default encapsulation mode and register with IP-in-IP encapsulation.

Note If an encapsulation type is configured on an interface using the **ip mobile router-service tunnel mode**command, that encapsulation type overrides the global encapsulation type configured with the **tunnel mode gre**command on that interface only. If there is no interface-level configuration, the interface inherits the global configuration.

Once GRE encapsulation is enabled, GRE keepalives can be configured on an interface using the **keepalive** command. GRE keepalives check for a failure in the end-to-end tunnel at a configurable interval. If the connection to the HA is lost, the mobile router will attempt to reregister. GRE keepalives must be configured on the mobile router only--no configuration is required on the HA.

Note If the GRE keepalive messages time out, indicating an interruption in the end-to-end tunnel, only the mobile router will tear down the GRE tunnel. The HA will not tear down its side of the tunnel.

Examples

The following example configures GRE encapsulation and GRE keepalive messages on an interface of a mobile router:

```
interface FastEthernet0/0
 ip address 10.52.52.2 255.255.255.0
 ip mobile router-service roam
 ip mobile router-service tunnel mode gre
!
interface tunnel 121
 keepalive 5 3
!
ip mobile router
 template tunnel 121
```

Related Commands

Command	Description
keepalive	Enables keepalive packets and specifies the number of times that the Cisco IOS software tries to send keepalive packets without a response before bringing down the interface or before bringing the tunnel protocol down for a specific interface.
tunnel mode gre	Sets the global encapsulation mode on all roaming interfaces of a mobile router to GRE.

ip mobile secure

To specify the mobility security associations for the mobile host, visitor, home agent, foreign agent, and proxy-host, use the **ip mobile secure** command in global configuration mode. To remove the mobility security associations, use the no form of this command.

ip mobile secure {**aaa-download| host| visitor| home-agent| foreign-agent| proxy-host**} {*lower-address* [*upper-address*]| **nai** *string*} {**inbound-spi** *spi-in* **outbound-spi** *spi-out*| **spi** *spi*} **key hex** *string* [**replay timestamp** [*number*] **algorithm** {**md5| hmac-md5**} **mode prefix-suffix**]

no ip mobile secure {**aaa-download| host| visitor| home-agent| foreign-agent| proxy-host**} {*lower-address* [*upper-address*]| **nai** *string*} {**inbound-spi** *spi-in* **outbound-spi** *spi-out*| **spi** *spi*} **key hex** *string* [**replay timestamp** [*number*] **algorithm** {**md5| hmac-md5**} **mode prefix-suffix**]

Syntax Description

aaa-download	Downloads security association from AAA at every timer interval.
host	Security association of the mobile host on the home agent.
visitor	Security association of the mobile host on the foreign agent.
home-agent	Security association of the remote home agent on the foreign agent.
foreign-agent	Security association of the remote foreign agent on the home agent.
proxy-host	Security association of the proxy Mobile IP users. This keyword is only available on Packet Data Serving Node (PDSN) platforms.
lower-address	IP address of a host or lower range of IP address pool.
upper-address	(Optional) Upper range of an IP address pool. If specified, security associations for multiple hosts are configured. The value used in the *upper-address* argument must be greater than that used in the *lower-address* argument.
nai *string*	Network access identifier of the mobile node. The **nai** *string* is valid only for a host, visitor, and proxy host.
inbound-spi *spi-in*	Security parameter index used for authenticating inbound registration packets. Range is from 0x100 to 0xffffffff.

outbound-spi *spi-out*	Security parameter index used for calculating the authenticator in outbound registration packets. Range is from 0x100 to 0xffffffff.
spi spi	Bidirectional SPI. Range is from 0x100 to 0xffffffff.
key hex *string*	ASCII string of hexadecimal values. No spaces are allowed.
replay	(Optional) Specifies replay protection used on registration packets.
timestamp	(Optional) Validates incoming packets to ensure that they are not being "replayed" by a spoofer using the timestamp method.
number	(Optional) Number of seconds. Registration is valid if received within the router's clock +/- 7 seconds. This means the sender and receiver are in time synchronization (NTP can be used).
algorithm	(Optional) Algorithm used to authenticate messages during registration.
md5	(Optional) Message Digest 5.
hmac-md5	(Optional) Hash-based message authentication code (HMAC) message digest 5.
mode	(Optional) Mode used to authenticate during registration.
prefix-suffix	(Optional) The key is used to wrap the registration information for authentication (for example, key registration information key) to calculate the message digest.

Command Default

No security association is specified.

Command Modes

Global configuration

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2	The *lower-address* and *upper-address* arguments were added.

Release	Modification
12.2(2)XC	The **nai** keyword was added.
12.2(13)T	The **hmac-md5** keyword was added and this commandwas integrated into Cisco IOS Release 12.2(13)T.
12.3(4)T	The **proxy-host** keyword was added for PDSN platforms.

Usage Guidelines

The security association consists of the entity address, SPI, key, replay protection method, authentication algorithm, and mode.

The SPI is the 4-byte index that selects the specific security parameters to be used to authenticate the peer. The security parameters consist of the authentication algorithm and mode, replay attack protection method, timeout, and IP address.

The HMAC-MD5 authentication algorithm is mandatory for mobile-home authentication (MHAE), mobile-foreign authentication (MFAE), and foreign-home authentication (FHAE)

On a home agent, the security association of the mobile host is mandatory for mobile host authentication. If desired, configure a foreign agent security association on your home agent. On a foreign agent, the security association of the visiting mobile host and security association of the home agent are optional. Multiple security associations for each entity can be configured.

If registration fails because the **timestamp** value is out of bounds, the time stamp of the home agent is returned so that the mobile node can reregister with the time-stamp value closer to that of the home agent, if desired.

The **nai** keyword is valid only for a host, visitor, and proxy host.

The **proxy-host** keyword is available only on PDSN platforms running specific PDSN code images; consult Feature Navigator for your Cisco IOS software release.

Note NTP is not required for operation but NTP can be used to synchronize time for all parties.

Examples

The following example shows mobile node 10.0.0.4, which has a key that is generated by the MD5 hash of the string:

```
ip mobile secure host 10.0.0.4 spi 100 key hex 12345678123456781234567812345678
```

Related Commands

Command	Description
ip mobile host	Configures the mobile host or mobile node group.
ip mobile proxy-host	Configures the proxy Mobile IP attributes.
ntp server	Allows the system clock to be synchronized by a time server.

Command	Description
show ip mobile secure	Displays the mobility security associations for mobile host, mobile visitor, foreign agent, or home agent.

ip mobile secure aaa-download

To specify that authentication, authorization, and account ing (AAA) mobility security associations (SAs) are downloaded from the AAA server and the rate at which the information is downloaded, use the **ip mobile secure aaa-downloa d** command in global configuration mode. To delete the AAA download rate, use the no form of this command.

ip mobile secure aaa-download rate *seconds*

no ip mobile secure aaa-download rate *seconds*

Syntax Description

rate	Rate at which the AAA SA is downloaded. • *seconds--Download rate, in seconds.* The range is from 1 to 100.

Command Default

No AAA SAs are downloaded.

Command Modes

Global configuration

Command History

Release	Modification
12.0(1)T	This command was introduced.

Usage Guidelines

SAs are downloaded from a AAA server on the first use. This command allows the home agent (HA) to prepopulate an SA table.

Examples

The following example shows a download rate of 35 seconds:

```
ip mobile secure aaa-download rate 35
```

Related Commands

Command	Description
ip mobile host	Configures the mobile host or mobile node group.
ip mobile proxy-host	Configures the proxy Mobile IP attributes.
ip mobile secure foreign-agent	Configures the mobility SAs for an FA.

Command	Description
ip mobile secure home-agent	Configures the mobility SAs for an HA.
ip mobile secure host	Configures the mobility SAs for a mobile host.
ip mobile secure mn-aaa	Specifies non-standard SPI values in the MN-AAA authentication extension that need to be accepted by the home agent or the foreign agent.
ip mobile secure proxy-host	Configures the mobility SAs for a proxy host.
ip mobile secure visitor	Configures the mobility SAs for a visitor.
ntp server	Allows the system clock to be synchronized by a time server.
show ip mobile secure	Displays the mobility SAs for a mobile host, mobile visitor, FA, or HA.

ip mobile secure foreign-agent

To specify the mobility security associations (SAs) for a foreign agent (FA), use the **ip mobile secure foreign-agent** command in global configuration mode. To remove the mobility SAs, use the no form of this command.

ip mobile secure foreign-agent *lower-address* [*upper-address*] {**inbound-spi** {*hex-in*| **decimal** *decimal-in*} **outbound-spi** {*hex-out*| **decimal** *decimal-out*}| **spi** {*hex-value*| **decimal** *decimal-value*}} **key** {**ascii** *string*| **hex** *string*} [**replay timestamp within** *seconds*] [**algorithm** {**hmac-md5**| **md5 mode prefix-suffix**}]

no ip mobile secure foreign-agent *lower-address* [*upper-address*] {**inbound-spi** {*hex-in*| **decimal** *decimal-in*} **outbound-spi** {*hex-out*| **decimal** *decimal-out*}| **spi** {*hex-value*| **decimal** *decimal-value*}}

Syntax Description

lower-address	IP address of an FA or lower range of IP address pool. *upper-address* --(Optional) Upper range of IP address pool. If specified, SAs for multiple FAs are configured. The *upper-address* value must be greater than the *lower-address* value.
inbound-spi	Bidirectional 4-byte security parameter index (SPI) used for authenticating inbound registration packets. *hex-in* --Index for inbound registration packets. The range is from 100 to ffffffff.
decimal	Decimal SPI. The arguments are as follows: *decimal-in* --SPI expressed as a decimal number for inbound registration packets. The range is from 256 to 4294967295. *decimal-out* --SPI expressed as a decimal number for outbound registration packets. The range is from 256 to 4294967295.
outbound-spi	SPI used for calculating the authenticator in outbound registration packets. *hex-out* --Index for outbound registration packets. The range is from 100 to ffffffff.

spi	SPI authenticates a peer. The argument and keyword are as follows: *hex-value* --SPI expressed as a hexadecimal number. The range is from 100 to ffffffff. Cisco recommends that you use hexadecimal values instead of decimal values for interoperability. **decimal--** Decimal SPI. The argument is as follows: *decimal-value* --SPI expressed as a decimal number. The range is from 256 to 4294967295.
key	Security key. The arguments and keywords are as follows: **ascii** *string* --Security key expressed as an ASCII string. A maximum of 32 characters is allowed. No spaces are allowed. **hex** *string* --Security key expressed in hexadecimal digits. A maximum of 32 hex digits is allowed. The range is from 100 to ffffffff. No spaces are allowed.
replay timestamp within	(Optional) Specifies the number of seconds that the router uses for replay protection. *seconds*-- Time, in seconds, that a router uses for replay protection. The range is from plus or minus 255. The default is plus or minus 7. The registration packet is considered “not replayed” if the time stamp in the packet is within plus or minus the configured number of seconds of the router clock.
algorithm	(Optional) Algorithm used to authenticate messages during registration. The keywords are as follows: **hmac-md5** --Hash-based Message Authentication Code (HMAC) MD5. The HMAC-MD5 authentication algorithm or MD5 (prefix-suffix) authentication algorithm is mandatory for mobile-home authentication (MHAE), mobile-foreign authentication (MFAE), or foreign-home authentication (FHAE). **md5 mode** --Message Digest 5 (MD5)mode used to authenticate packets during registration. **prefix-suffix** --Wrapped registration information for authentication (for example, key registration information key) that calculates the message digest. Cisco no longer recommends this method of authentication, but it is retained for backward compatibility.

Command Default

No SA is specified for FAs.

Command Modes

Global configuration

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2	The *lower-address* and *upper-address* arguments were added.
12.2(13)T	The **hmac-md5** keyword was added.

Usage Guidelines

The SA consists of an entity address, SPI, key, replay protection method, authentication algorithm, and authentication algorithm mode (prefix-suffix).

On a FA, the SA of the visiting mobile host and the SA of the home agent (HA) are optional. Multiple SAs for each entity can be configured.

The SA of a visiting mobile host on the MFAE and the SA of the HA on the FHAE are optional on the FA as long as they are not specified on the other entity. Multiple SAs for each entity can be configured.

Note NTP is not required for operation, but NTP can be used to synchronize time for all parties.

Examples

The following example shows the configuration of an FA with an IP address of 209.165.200/254:

```
ip mobile secure foreign-agent 209.165.200/254 inbound-spi 203 outbound-spi 150 key hex
ffffffff
```

Related Commands

Command	Description
ip mobile host	Configures the mobile host or mobile node group.
ip mobile proxy-host	Configures the proxy Mobile IP attributes.
ip mobile secure aaa-download	Configures the rate at which AAA security associations are downloaded.
ip mobile secure home-agent	Configures the mobility SAs for an HA.
ip mobile secure host	Configures the mobility SAs for a mobile host.

Command	Description
ip mobile secure mn-aaa	Specifies non-standard SPI values in the MN-AAA authentication extension that need to be accepted by the home agent or foreign agent.
ip mobile secure proxy-host	Configures the mobility SAs for a proxy host.
ip mobile secure visitor	Configures the mobility SAs for a visitor.
show ip mobile secure	Displays the mobility SAs for a mobile host, mobile visitor, FA, or HA.

ip mobile secure home-agent

To specify the mobility security associations (SAs) for a home agent (HA), use the **ip mobile secure** home-agent command in global configuration mode. To remove the mobility SAs, use the no form of this command.

ip mobile secure home-agent *lower-address* [*upper-address*] {**inbound-spi** {*hex-in*| **decimal** *decimal-in*} **outbound-spi** {*hex-out*| **decimal** *decimal-out*}| **spi** {*hex-value*| **decimal** *decimal-value*}} **key** {**ascii** *string*| **hex** *string*} [**replay timestamp within** *seconds*] [**algorithm** {**hmac-md5**| **md5 mode prefix-suffix**}] **[ignore-spi]**

no ip mobile secure home-agent *lower-address* [*upper-address*] {**inbound-spi** {*hex-in*| **decimal** *decimal-in*} **outbound-spi** {*hex-out*| **decimal** *decimal-out*}| **spi** {*hex-value*| **decimal** *decimal-value*}}

Syntax Description

lower-address	IP address of an HA or lower range of IP address pool. *upper-address* --(Optional) Upper range of IP address pool. If specified, SAs for multiple HAs are configured. The *upper-address* value must be greater than the *lower-address* value.
inbound-spi	Bidirectional 4-byte security parameter index (SPI) used for authenticating inbound registration packets. *hex-in* --Index for inbound registration packets. The range is from 100 to ffffffff.
decimal	Decimal SPI. The arguments are as follows: *decimal-in* --SPI expressed as a decimal number for inbound registration packets. The range is from 256 to 4294967295. *decimal-out* --SPI expressed as a decimal number for outbound registration packets. The range is from 256 to 4294967295.
outbound-spi	SPI used for calculating the authenticator in outbound registration packets. *hex-out* --Index for outbound registration packets. The range is from 100 to ffffffff.

spi	SPI authenticates a peer. The argument and keyword are as follows: *hex-value* --SPI expressed as a hexadecimal number. The range is from 100 to ffffffff. Cisco recommends that you use hexadecimal values instead of decimal values for interoperability. **decimal--** Decimal SPI. The argument is as follows: *decimal-value* --SPI expressed as a decimal number. The range is from 256 to 4294967295.
key	Security key. The arguments and keywords are as follows: **ascii** *string* --Security key expressed as an ASCII string. A maximum of 32 characters is allowed. No spaces are allowed. **hex** *string* --Security key expressed in hexadecimal digits. A maximum of 32 hex digits is allowed. The range is from 100 to ffffffff. No spaces are allowed.
replay timestamp within	(Optional) Specifies the number of seconds that the router uses for replay protection. *seconds--* Time, in seconds, that a router uses for replay protection. The range is from plus or minus 255. The default is plus or minus 7. The registration packet is considered “not replayed” if the time stamp in the packet is within plus or minus the configured number of seconds of the router clock.
algorithm	(Optional) Algorithm used to authenticate messages during registration. The keywords are as follows: **hmac-md5** --Hash-based Message Authentication Code (HMAC) MD5. The HMAC-MD5 authentication algorithm or MD5 (prefix-suffix) authentication algorithm is mandatory for mobile-home authentication (MHAE), mobile-foreign authentication (MFAE), or foreign-home authentication (FHAE). **md5 mode** --Message Digest 5 (MD5)mode used to authenticate packets during registration. **prefix-suffix** --Wrapped registration information for authentication (for example, key registration information key) that calculates the message digest. Cisco no longer recommends this method of authentication, but it is retained for backward compatibility.

ignore-spi	(Optional) Allows authentications that ignore SPI.

Command Default

No SA is specified for HAs.

Command Modes

Global configuration

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2	The *lower-address* and *upper-address* arguments were added.
12.2(13)T	The **hmac-md5** keyword was added.

Usage Guidelines

The SA consists of an entity address, SPI, key, replay protection method, authentication algorithm, and authentication algorithm mode (prefix-suffix).

The HA may have multiple SAs for each peer. The SPI specifies which SA to use for the peer and selects the specific security parameters to be used to authenticate the peer.

On an HA, the SA of the mobile host is mandatory for mobile host authentication and allows the HA to compute the MHAE for mobile host authentication. If desired, configure a foreign agent (FA) SA on your HA.

The mobile IP protocol automatically synchronizes the time stamp used by the mobile node (MN) in its registration requests. If the MN registration request time stamp is outside the HA permitted replay protection time interval, the HA will respond with the number of seconds by which the MN time stamp is off relative to the HA clock. This allows the MN to adjust its time stamp and use synchronized time stamps in subsequent registration attempts.

If you prefer that the MN first registration attempt always fall within the HA replay protection time interval, use Network Time Protocol (NTP) to synchronize the MN and HA.

Note NTP is not required for operation, but NTP can be used to synchronize time for all parties.

Examples

The following example shows the configuration of an SA for an HA with an IP address of 10.0.0.4:

```
ip mobile secure home-agent 10.0.0.4 spi 100 key hex ffffffff
```

Related Commands

Command	Description
ip mobile host	Configures the mobile host or mobile node group.

Command	Description
ip mobile proxy-host	Configures the proxy Mobile IP attributes.
ip mobile secure aaa-download	Configures the rate at which AAA security associations are downloaded.
ip mobile secure foreign-agent	Configures the mobility SAs for an FA.
ip mobile secure host	Configures the mobility SAs for a mobile host.
ip mobile secure mn-aaa	Specifies non-standard SPI values in the MN-AAA authentication extension that need to be accepted by the home agent or foreign agent.
ip mobile secure proxy-host	Configures the mobility SAs for a proxy host.
ip mobile secure visitor	Configures the mobility SAs for a visitor.
ntp server	Allows the system clock to be synchronized by a time server.
show ip mobile secure	Displays the mobility SAs for a mobile host, mobile visitor, FA, or HA.

ip mobile secure host

To specify the mobility security associatio ns (SAs) for a mobile host, use the **ip mobile secure host** command in global configuration mode. To remove the mobility SAs, use the no form of this command.

ip mobile secure host {**l** *ower-address* [*upper-address*]| **nai** *nai-string*} {**inbound-spi** {*hex-in*| **decimal** *decimal-in*} **outbound-spi** {*hex-out*| **decimal** *decimal-out*}| **spi** {*hex-value*| **decimal** *decimal-value*}} **key** {**ascii** *string*| **hex** *string*} [**replay timestamp within** *seconds*] [**algorithm** {**hmac-md5**| **md5 mode prefix-suffix**}]

no mobile secure host {*lower-address* [*upper-address*]| **nai** *nai-string*} {**inbound-spi** {*hex-in*| **decimal** *decimal-in*} **outbound-spi** {*hex-out*| **decimal** *decimal-out*}| **spi** {*hex-value*| **decimal** *decimal-value*}}

Syntax Description

lower-address	IP address of a host or lower range of IP address pool. • *upper-address* --(Optional) Upper range of IP address pool. If specified, SAs for multiple hosts are configured. **Note** The *upper-address* value must be greater than the *lower-address* value.
nai	Network access identifier (NAI) of the mobile node (MN). • *nai-string* --NAI username or username@realm.
inbound-spi	Bidirectional 4-byte security parameter index (SPI) used for authenticating inbound registration packets. • *hex-in* --Index for inbound registration packets. The range is from 100 to ffffffff.
decimal	Decimal SPI. The arguments are as follows: • *decimal-in* --SPI expressed as a decimal number for inbound registration packets. The range is from 256 to 4294967295. • *decimal-out* --SPI expressed as a decimal number for outbound registration packets. The range is from 256 to 4294967295.
outbound-spi	SPI used for calculating the authenticator in outbound registration packets. • *hex-out* --Index for outbound registration packets. The range is from 100 to ffffffff.

spi	SPI authenticates a peer. The argument and keyword are as follows: • *hex-value* --SPI expressed as a hexadecimal number. The range is from 100 to ffffffff. **Note** Cisco recommends that you use hexadecimal values instead of decimal values for interoperability. • **decimal--** Decimal SPI. The argument is as follows: • *decimal-value*--SPI expressed as a decimal number. The range is from 256 to 4294967295.
key	Security key. The arguments and keywords are as follows: • **ascii** *string* --Security key expressed as an ASCII string. A maximum of 32 characters is allowed. No spaces are allowed. • **hex** *string* --Security key expressed in hexadecimal digits. A maximum of 32 hex digits is allowed. The range is from 100 to ffffffff. No spaces are allowed.
replay timestamp within	(Optional) Specifies the number of seconds that the router uses for replay protection. • *seconds*-- Time, in seconds, that a router uses for replay protection. The range is from plus or minus 255. The default is plus or minus 7. **Note** The registration packet is considered “not replayed” if the time stamp in the packet is within plus or minus the configured number of seconds of the router clock.

algorithm	(Optional) Algorithm used to authenticate messages during registration. The keywords are as follows: • **hmac-md5** --Hash-based Message Authentication Code (HMAC) MD5. **Note** The HMAC-MD5 authentication algorithm or MD5 (prefix-suffix) authentication algorithm is mandatory for mobile-home authentication (MHAE), mobile-foreign authentication (MFAE), or foreign-home authentication (FHAE). • **md5 mode** --Message Digest 5 (MD5)mode used to authenticate packets during registration. • **prefix-suffix** --Wrapped registration information for authentication (for example, key registration information key) that calculates the message digest. **Note** Cisco no longer recommends this method of authentication, but it is retained for backward compatibility.

Command Default

No SA is specified for mobile hosts.

Command Modes

Global configuration

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2	The *lower-address* and *upper-address* arguments were added.
12.2(2)XC	The **nai** keyword was added.
12.2(13)T	The **hmac-md5** keyword was added.

Usage Guidelines

The SA consists of an entity address, SPI, key, replay protection method, authentication algorithm, and authentication algorithm mode (prefix-suffix).

The SA of a visiting mobile host on the MFAE and the SA of the home agent (HA) on the FHAE are optional as long as they are not specified on the other entity. Multiple SAs for each entity can be configured.

The HMAC-MD5 authentication algorithm is mandatory for MHAE, MFAE, and FHAE.

Note NTP is not required for operation, but NTP can be used to synchronize time for all parties.

Examples

The following example shows the configuration of an SA for a host:

```
ip mobile secure host 10.0.0.4 spi 100 key hex 12345678123456781234567812345678
```

Related Commands

Command	Description
ip mobile host	Configures the mobile host or mobile node group.
ip mobile proxy-host	Configures the proxy Mobile IP attributes.
ip mobile secure aaa-download	Configures the rate at which AAA security associations are downloaded.
ip mobile secure foreign-agent	Configures the mobility SAs for an FA.
ip mobile secure home-agent	Configures the mobility SAs for an HA.
ip mobile secure mn-aaa	Specifies non-standard SPI values in the MN-AAA authentication extension that need to be accepted by the home agent or foreign agent.
ip mobile secure proxy-host	Configures the mobility SAs for a proxy host.
ip mobile secure visitor	Configures the mobility SAs for a visitor.
ntp server	Allows the system clock to be synchronized by a time server.
show ip mobile secure	Displays the mobility SAs for a mobile host, mobile visitor, FA, or HA.

ip mobile secure mn-aaa

To specify non-standard security parameter index (SPI) values in the MN-AAA authentication extension that need to be accepted by the home agent or the foreign agent, use the **ip mobile secure mn-aaa** command in global configuration mode. To disable this functionality, use the no form of this command.

ip mobile secure mn-aaa spi {*hex-value*| **decimal** *decimal-value*} **algorithm md5 mode ppp-chap-style**

no ip mobile secure mn-aaa spi {*hex-value*| **decimal** *decimal-value*} **algorithm md5 mode ppp-chap-style**

Syntax Description

spi	Bidirectional security parameter index (SPI). The index can be a hexadecimal or decimal value. The arguments and keyword are as follows: *hex -value*--SPI expressed in hexadecimal digits. The range is from 100 to ffffffff. No spaces are allowed. The maximum is 32 characters. **decimal** *decimal-value* --SPI expressed as a decimal number. The range is from 256 to 4294967295. No spaces are allowed. The maximum is 32 characters.
algorithm md5 mode ppp-chap-style	Message Digest 5 (MD5) authentication algorithm used during authentication by the Challenge-Handshake Authentication Protocol (CHAP).

Command Default

The home agent or foreign agent only accept the standard SPI value in the MN-AAA authentication extension that specifes CHAP-style authentication using MD5. The standard value for the SPI is 2.

Command Modes

Global configuration

Command History

Release	Modification
12.2	This command was introduced.

Usage Guidelines

The SPI is the 4-byte index that selects the specific security parameters to be used to authenticate the peer. The security parameters consist of the authentication algorithm and mode.

A mobile node configured to be authenticated via an MN-AAA authentication extension is required to use an SPI value of 2 to indicate CHAP-style authentication using MD5 as specified by RFC 3012, *Mobile IPv4 Challenge/Response Extensions.*

Some network implementations need the flexibility to allow an SPI value other than 2 even though the mobile node is authenticated using CHAP. The **ip mobile secure mn-aaa** command maps new SPI values in the MN-AAA extension of the registration message to the SPI value pre-defined by RFC 3012. When a registration request arrives at the foreign agent or home agent with the MN-AAA extension containing an SPI value specified by the **ip mobile secure mn-aaa** command, the foreign agent or home agent will process it as if the value was 2 instead of rejecting the request.

Use this command with caution because it is non-standard behavior. For example, different vendors might use the same non-standard SPI to denote different authentication methods and this could affect interoperability. Cisco recommends the use of standard SPI values if possible to be used in the MN-AAA authentication extension by the mobile node.

Examples

In the following example, the foreign agent or home agent will process the registration request even though the CHAP SPI value is not 2:

```
ip mobile secure mn-aaa spi 1234 algorithm md5 mode ppp-chap-style
```

ip mobile secure proxy-host

To specify the mobility security assoc iations (SAs) for a proxy host, use the **ip mobile secure proxy-host** command in global configuration mode. To remove the mobility SAs, use the no form of this command.

ip mobile secure proxy-host {*lower-address* [*upper-address*]| **nai** *nai-string*} {**inbound-spi** *spi-in* **outbound-spi** *spi-out*| **spi** {*hex-value*| **decimal** *decimal-value*}} *key* {**ascii** *string*| **hex** *string*} [**replay timestamp** *seconds*] [**algorithm** {**md5 mode prefix-suffix| hmac-md5**}]

no ip mobile secure proxy-host {*lower-address* [*upper-address*]| **nai** *nai-string*} {**inbound-spi** *spi-in* **outbound-spi** *spi-out*| **spi** {*hex-value*| **decimal** *decimal-value*}} **key** {**ascii** *string*| **hex** *string*} [**replay timestamp** *seconds*] [**algorithm** {**md5 mode prefix-suffix| hmac-md5**}]

Syntax Description

lower-address	IP address of a proxy host or lower range of IP address pool. *upper-address* --(Optional) Upper range of IP address pool. If specified, SAs for multiple proxy hosts are configured. The *upper-address* value must be greater than the *lower-address* value.
nai	Network access identifier (NAI) of the mobile node (MN). *nai-string* --NAI username or username@realm.
inbound-spi	Bidirectional 4-byte security parameter index (SPI) used for authenticating inbound registration packets. *spi-in* --Index for inbound registration packets. The range is from 100 to ffffffff.
outbound-spi	SPI used for calculating the authenticator in outbound registration packets. *spi-out* --Index for outbound registration packets. The range is from 100 to ffffffff.
spi	SPI authenticates a peer. The argument and keyword are as follows: *hex-value* --SPI expressed as a hexadecimal number. The range is from 100 to ffffffff. Cisco recommends that you use hexadecimal values instead of decimal values for interoperability. **decimal--** Decimal SPI. The argument is as follows: *decimal-value* --SPI expressed as a decimal number. The range is from 256 to 4294967295.

key	Security key. The arguments and keywords are as follows: **ascii** *string* --Security key expressed as an ASCII string. A maximum of 32 characters is allowed. No spaces are allowed. **hex** *string* --Security key expressed in hexadecimal digits. A maximum of 32 hex digits is allowed. The range is from 100 to ffffffff. No spaces are allowed.
replay timestamp	(Optional) Specifies the number of seconds that the router uses for replay protection. *seconds*-- Time, in seconds, that a router uses for replay protection. The range is from plus or minus 255. The default is plus or minus 7. The registration packet is considered "not replayed" if the time stamp in the packet is within plus or minus the configured number of seconds of the router clock.
algorithm	(Optional) Algorithm used to authenticate messages during registration. The keywords are as follows: **md5 mode** --Message Digest 5 (MD5)mode used to authenticate packets during registration. **prefix-suffix** --Wrapped registration information for authentication (for example, key registration information key) that calculates the message digest. Cisco no longer recommends this method of authentication, but it is retained for backward compatibility. **hmac-md5** --Hash-based Message Authentication Code (HMAC) MD5. The HMAC-MD5 authentication algorithm or MD5 (prefix-suffix) authentication algorithm is mandatory for mobile-home authentication (MHAE), mobile-foreign authentication (MFAE), or foreign-home authentication (FHAE).

Command Default

No SA is specified for proxy hosts.

Command Modes

Global configuration

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2	The *lower-address* and *upper-address* arguments were added.
12.2(2)XC	The **nai** keyword was added.
12.2(13)T	The **hmac-md5** keyword was added.
12.3(4)T	The **proxy-host** keyword was added for Packet Data Serving Node (PDSN) platforms only.

Usage Guidelines

The SA consists of an entity address, SPI, key, replay protection method, authentication algorithm, and authentication algorithm mode (prefix-suffix).

The HMAC-MD5 authentication algorithm is mandatory for MHAE, MFAE, and FHAE.

Note The **proxy-host** keyword is available only on PDSN platforms that are running specific PDSN code images; consult Cisco Feature Navigator for your Cisco IOS software release.

Note NTP is not required for operation, but NTP can be used to synchronize time for all parties.

Examples

The following example shows the configuration of SAs for a proxy host:

```
ip mobile secure proxy-host 10.0.0.4 spi 100 key hex 12345678123456781234567812345678
```

Related Commands

Command	Description
ip mobile host	Configures the mobile host or mobile node group.
ip mobile proxy-host	Configures the proxy Mobile IP attributes.
ip mobile secure aaa-download	Configures the rate at which AAA security associations are downloaded.
ip mobile secure foreign-agent	Configures the mobility SAs for an FA.
ip mobile secure home-agent	Configures the mobility SAs for an HA.
ip mobile secure host	Configures the mobility SAs for a mobile host.

Command	Description
ip mobile secure mn-aaa	Specifies non-standard SPI values in the MN-AAA authentication extension that need to be accepted by the home agent or the foreign agent.
ip mobile secure visitor	Configures the mobility SAs for a visitor.
ntp server	Allows the system clock to be synchronized by a time server.
show ip mobile secure	Displays the mobility SAs for a mobile host, mobile visitor, FA, or HA.

ip mobile secure visitor

To specify the mobility security associations (SAs) for a visitor, use the **ip mobile secure visitor** command in global configuration mode. To remove the mobility security associations, use the no form of this command.

ip mobile secure visitor {*lower-address* [*upper-address*]| **nai** *nai-string*} {**inbound-spi** *spi-in* **outbound-spi** *spi-out*| **spi** {*hex-value*| **decimal** *decimal-value*}} **key** {**ascii** *string*| **hex** *string*} [**replay timestamp** *seconds*] [**algorithm** {**md5 mode prefix-suffix**| **hmac-md5**}]

no ip mobile secure visitor {*lower-address* [*upper-address*]| **nai** *nai-string*} {**inbound-spi** *spi-in* **outbound-spi** *spi-out*| **spi** {*hex-value*| **decimal** *decimal-value*}} **key** {**ascii** *string*| **hex** *string*} [**replay timestamp** *seconds*] [**algorithm** {**md5 mode prefix-suffix**| **hmac-md5**}]

Syntax Description

lower-address	IP address of a visitor or lower range of IP address pool. *upper-address* --(Optional) Upper range of IP address pool. If specified, SAs for multiple visitors are configured. The *upper-address* value must be greater than the *lower-address* value.
nai	Network access identifier (NAI) of the mobile node (MN). *nai-string* --NAI username or username@realm.
inbound-spi	Bidirectional 4-byte security parameter index (SPI) used for authenticating inbound registration packets. *spi-in* --Index for inbound registration packets. The range is from 100 to ffffffff.
outbound-spi	SPI used for calculating the authenticator in outbound registration packets. *spi-out* --Index for outbound registration packets. The range is from 100 to ffffffff.
spi	SPI authenticates a peer. The argument and keyword are as follows: *hex-value* --SPI expressed as a hexadecimal number. The range is from 100 to ffffffff. Cisco recommends that you use hexadecimal values instead of decimal values for interoperability. **decimal--** Decimal SPI. The argument is as follows: *decimal-value* --SPI expressed as a decimal number. The range is from 256 to 4294967295.

key	Security key. The arguments and keywords are as follows: **ascii** *string* --Security key expressed as an ASCII string. A maximum of 32 characters is allowed. No spaces are allowed. **hex** *string* --Security key expressed in hexadecimal digits. A maximum of 32 hex digits is allowed. The range is from 100 to ffffffff. No spaces are allowed.
replay timestamp	(Optional) Specifies the number of seconds that the router uses for replay protection. *seconds*-- Time, in seconds, that a router uses for replay protection. The range is from plus or minus 255. The default is plus or minus 7. The registration packet is considered “not replayed” if the time stamp in the packet is within plus or minus the configured number of seconds of the router clock.
algorithm	(Optional) Algorithm used to authenticate messages during registration. The keywords are as follows: **md5 mode** --Message Digest 5 (MD5)mode used to authenticate packets during registration. **prefix-suffix** --Wrapped registration information for authentication (for example, key registration information key) that calculates the message digest. Cisco no longer recommends this method of authentication, but it is retained for backward compatibility. **hmac-md5** --Hash-based Message Authentication Code (HMAC) MD5. The HMAC-MD5 authentication algorithm or MD5 (prefix-suffix) authentication algorithm is mandatory for mobile-home authentication (MHAE), mobile-foreign authentication (MFAE), or foreign-home authentication (FHAE).

No SA is specified for visitors.

Command Modes

Global configuration

Command History

Release	Modification
12.0(1)T	This command was introduced.

Release	Modification
12.2	The *lower-address* and *upper-address* arguments were added.
12.2(2)XC	The **nai** keyword was added.
12.2(13)T	The **hmac-md5** keyword was added.

Usage Guidelines

The SA consists of an entity address, SPI, key, replay protection method, authentication algorithm, and authentication algorithm mode (prefix-suffix).

The SA of a visiting mobile host on the MFAE and the SA of the home agent (HA) on the FHAE are optional as long as they are not specified on the other entity. Multiple SAs for each entity can be configured.

The mobile IP protocol automatically synchronizes the time stamp used by the MN in its registration requests. If the MN registration request time stamp is outside the visitor permitted replay protection time interval, the visitor will respond with the number of secondsby which the MN time stamp is off relative to the visitor clock. This allows the MN to adjust its time stamp and use synchronized time stamps in subsequent registration attempts.

If you prefer that the MN first registration attempt always fall within the visitor replay protection time interval, use Network Time Protocol (NTP) to synchronize the MN and visitor.

The HMAC-MD5 authentication algorithm is mandatory for MHAE, MFAE, and FHAE.

Note NTP is not required for operation, but NTP can be used to synchronize time for all parties.

Examples

The following example shows the configuration of SAs for a visitor:

```
ip mobile secure visitor 10.0.0.4 spi 100 key hex 12345678123456781234567812345678
```

Related Commands

Command	Description
ip mobile host	Configures the mobile host or mobile node group.
ip mobile proxy-host	Configures the proxy Mobile IP attributes.
ip mobile secure aaa-download	Configures the rate at which AAA security associations are downloaded.
ip mobile secure foreign-agent	Configures the mobility SAs for an FA.
ip mobile secure home-agent	Configures the mobility SAs for an HA.
ip mobile secure host	Configures the mobility SAs for a mobile host.

Command	Description
ip mobile secure mn-aaa	Specifies non-standard SPI values in the MN-AAA authentication extension that need to be accepted by the home agent or the foreign agent.
ip mobile secure proxy-host	Configures the mobility SAs for a proxy host.
ntp server	Allows the system clock to be synchronized by a time server.
show ip mobile secure	Displays the mobility SAs for a mobile host, mobile visitor, FA, or HA.

ip mobile tunnel

To specify the settings of tunnels created by Mobile IP, use the **ip mobile tunnel**command in global configuration mode. To disable the setting of tunnels created by Mobile IP, use the **no** form of this command.

ip mobile tunnel {**crypto map** *map-name*| **route-cache [cef]**| **path-mtu-discovery** [**age-timer** {*minutes*| **infinite**}]| **nat** {**inside**| **outside**}| **route-map** *map-tag*}

no ip mobile tunnel {**crypto map** *map-name*| **route-cache [cef]**| **path-mtu-discovery** [**age-timer** {*minutes*| **infinite**}]| **nat** {**inside**| **outside**}| **route-map** *map-tag*}

Syntax Description

crypto map	Enables encryption or decryption on new tunnels. This keyword is only available on platforms running specific Packet Data Serving Node (PDSN) code images.
map-name	The name of the crypto map. This argument is available only on platforms running specific PDSN code images.
route-cache	Sets tunnels to fast-switching mode.
cef	Sets tunnels to Cisco Express Forwarding (CEF) switching mode if CEF is enabled on the router.
path-mtu-discovery	Specifies when the tunnel MTU should expire if set by Path MTU Discovery.
age-timer *minutes*	(Optional) Time interval in minutes after which the tunnel reestimates the path MTU.
infinite	(Optional) Turns off the age timer.
nat	Ap plies Network Address Translation (NAT) on the tunnel interface.
inside	Sets the dynamic tunnel as the inside interface for NAT.
outside	Sets the dynamic tunnel as the outside interface for NAT.
route-map *map-tag*	Defines a meaningful name for the route map.

Command Default

Disabled.

If enabled, default value for the *minutes* argument is 10 minutes.

Command Modes

Global configuration

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.1(1)T	The **nat**, **inside**, and **outside**keywords were added.
12.2T	The **cef** keyword was added.
12.2(13)T	The **route-map**keyword and *map-tag* argument were added.
12.3(4)T	The **crpto map** keyword and *map-name* argument were added for PDSN platforms.

Usage Guidelines

Path MTU Discovery is used by end stations to find a packet size that does not need to be fragmented when being sent between the end stations. Tunnels must adjust their MTU to the smallest MTU interior to achieve this condition, as described in RFC 2003.

The discovered tunnel MTU should be aged out periodically to possibly recover from a case where suboptimum MTU existed at time of discovery. It is reset to the outgoing MTU of the interface.

The **no ip mobile tunnel route-cache** command disables fast switching and CEF switching (if CEF is enabled) on Mobile IP tunnels. The **no ip mobile tunnel route-cache cef** command disables CEF switching only.

CEF switching is currently not supported on a foreign agent when reverse tunneling is enabled. If reverse tunneling is enabled at the foreign agent, disable CEF on the foreign agent using the **no ip cef** global configuration command. If the foreign agent does not support reverse tunneling, there is no need to disable CEF at the global configuration level.

The **crypto map** *map-name*keyword and argumentcombination are available only on platforms running specific PDSN code images; consult Feature Navigator for your Cisco IOS software release.

Examples

The following example sets the discovered tunnel MTU to expire in 10 minutes (600 seconds):

```
ip mobile tunnel path-mtu-discovery age-timer 600
```

Related Commands

Command	Description
ip cef	Enables CEF on the RP card.
show ip mobile tunnel	Displays active tunnels.

ip mobile virtual-network

To define a virtual network, use the **ip mobile virtual-network** command in global configuration mode. To remove the virtual network, use the **no** form of this command.

ip mobile virtual-network *net mask* [**address** *address*]

no ip mobile virtual-network *net mask*

Syntax Description

net	Network associated with the IP address of the virtual network.
mask	Mask associated with the IP address of the virtual network.
address address	(Optional) IP address of a home agent on a virtual network.

Command Default

No home agent addresses are specified.

Command Modes

Global configuration

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.0(2)T	The **address**keyword and *address* argument were added.

Usage Guidelines

This command inserts the virtual network into the routing table to allow mobile nodes to use the virtual network as their home network. The network is propagated when redistributed to other routing protocols.

Note You may need to include virtual networks when configuring the routing protocols. If this is the case, use the **redistribute mobile** router configuration command to redistribute routes from one routing domain to another.

Examples

The following example adds the virtual network 20.0.0.0 to the routing table and specifies that the home agent IP address is configured on the loopback interface for that virtual network:

```
interface ethernet 0
 ip address 1.0.0.1 255.0.0.0
 standby ip 1.0.0.10
 standby name SanJoseHA
interface loopback 0
 ip address 20.0.0.1 255.255.255.255
ip mobile home-agent
 ip mobile virtual-network 20.0.0.0 255.255.0.0 address 20.0.0.1
 ip mobile home-agent standby SanJoseHA virtual-network
 ip mobile secure home-agent 1.0.0.2 spi 100 hex 00112233445566778899001122334455
```

Related Commands

Command	Description
ip mobile host	Configures the mobile host or mobile node group.
redistribute mobile	Redistributes routes from one routing domain into another routing domain.

ip mobile vpn-realm

To define the virtual private network (VPN) realms to be used in home agent policy routing, use the **ip mobile vpn-realm**command in global configuration mode. To remove the VPN realms, use the **no** form of this command.

ip mobile vpn-realm *realm-name* **route-map-sequence** *sequence-number*

no ip mobile vpn-realm *realm-name* **route-map-sequence** *sequence-number*

Syntax Description

realm-name	Network access identifier (NAI) realm name.
route-map-sequence	Sequence of the route map.
sequence-number	Number that indicates the position a new route map is to have in the list of route maps already configured with the same name. If given with the **no** form of this command, it specifies the position of the route map that should be deleted. The sequence number range is from 0 to 65535.

Command Default

No default behavior or values.

Command Modes

Global configuration

Command History

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

Usage Guidelines

The *sequence-number* argument must match that configured in the **route-map** *sequence-number* command.

Examples

The following example shows two realms configured on the router:

```
ip mobile vpn-realm company1.com route-map-sequence 20
ip mobile vpn-realm company2.com route-map-sequence 10
```

Related Commands

Command	Description
route map	Defines the conditions for redistributing routes from one routing protocol into another, or to enable policy routing.
show ip mobile vpn-realm	Displays VPN realms configured for Mobile IP.

ip mux

To enable IP multiplexing in IPv4 on an interface, use the **ip mux** command in interface configuration mode. To disable IP multiplexing on an interface, use the **no** form of the command.

ip mux

no ip mux

Syntax Description

This command has no arguments or keywords.

Command Default

IP multiplexing is disabled on the interface.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.2(2)GC	This command was introduced.
15.2(4)M	This command was integrated into Cisco IOS Release 15.2(4)M.

Usage Guidelines

IP multiplexing must be enabled on the interface before the interface can receive or send IP multiplexing superframes.

Examples

The following example shows how to configure IP multiplexing in IPv4 on FastEthernet interface 0/1.

```
Router# configure terminal
Router(config)# interface fastethernet0/1
Router(config-if)# ip address 192.0.2.1
Router(config-if)# ip mux
Router(config-if)# exit
Router(config)#
```

Related Commands

Command	Description
show mux interface	Displays configured IP multiplexing statistics for an interface.

ip mux cache

To set the IP multiplexing cache size in bytes, use the **ip mux cache** command in global configuration mode. To return to the default setting, use the **no** form of this command.

ip mux cache *size*

no ip mux cache *size*

Syntax Description

size	Maximum cache size in bytes. The range is 1,000,000 to 4,294,967,295.

Command Default

The default cache size is 1,000,000 bytes.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.2(2)GC	This command was introduced.
15.2(4)M	This command was integrated into Cisco IOS Release 15.2(4)M.

Usage Guidelines

If you do not enter a cache size, the IP multiplexing packet handler defaults to 1,000,000 bytes. A 1,000,000 byte cache contains 11,363 entries.

Examples

The following example shows how to configure the IP multiplexing cache size to 5,000,000:

```
Router# configure terminal
Router(config)# ip mux cache 5000000
Router(config)#
```

Related Commands

Command	Description
show mux cache	Displays IP multiplexing cache statistics.

ip mux policy

To create an IPv4 multiplexing differentiated services code point (DSCP) policy with a specified name, use the **ip mux policy** command in global configuration mode. To delete the IPv4 multiplexing policy, use the **no** form of this command.

ip mux policy *policy-name*

no ip mux policy *policy-name*

Syntax Description

policy-name	Name of the IPv4 multiplexing policy.

Command Default

No policies are created.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.2(2)GC	This command was introduced.
15.2(4)M	This command was integrated into Cisco IOS Release 15.2(4)M.

Usage Guidelines

You can specify up to three policies in addition to the default policy.

If you do not configure an IPv4 multiplexing policy, all IPv4 multiplexing packets are sent using the default IPv4 multiplexing policy with a DSCP value equal to 0.

Examples

The following example shows how to configure an IPv4 multiplexing DSCP policy with the name *routeRTP-SJ* and enter IPv4 multiplexing policy configuration mode:

```
Router# configure terminal
Router(config)# ip mux policy routeRTP-SJ
Router(config-ipmux-policy)#
```

Related Commands

Command	Description
show mux profile `	Displays multiplexing statistics and the sconfiguration for a specific IP multiplexing profile.

ip mux profile

To create an IPv4 multiplexing profile with a specified name, use the **ip mux profile** command in global configuration mode. To delete the IPv4 multiplexing profile, use the **no** form of this command.

ip mux profile *profile-name*

no ip mux profile *profile-name*

Syntax Description

profile-name	Name of the IPv4 multiplexing profile.

Command Default

No default profile exists.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.2(2)GC	This command was introduced.
15.2(4)M	This command was integrated into Cisco IOS Release 15.2(4)M.

Usage Guidelines

You can specify up to 500 profiles.

Examples

The following example shows how to configure an IPv4 multiplexing profile with the name *routeRTP-SJ* and enter IPv4 multiplexing profile configuration mode:

```
Router# configure terminal
Router(config)# ip mux profile routeRTP-SJ
Router(config-ipmux-profile)#
```

Related Commands

Command	Description
show mux profile	Displays multiplexing statistics and the configuration for a specific IP multiplexing profile.

ip mux udpport

To specify a destination UDP port to use for IPv4 multiplexed packets, use the **ip mux udpport** command in global configuration mode. To return to the default setting, use the **no** form of this command.

ip mux udpport *port-number*

no ip mux udpport

Syntax Description

port-number	UDP port number. The range is 1,024 to 49,151.

Command Default

The default port number is 6,682.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.2(2)GC	This command was introduced.
15.2(4)M	This command was integrated into Cisco IOS Release 15.2(4)M.

Usage Guidelines

If you do not enter a port number, the system uses the default port 6,682.

Examples

The following example shows how to configure the UDP port for IP multiplexed packets to 5,000:

```
Router# configure terminal
Router(config)# ip mux udpport 5000
Router(config)#
```

Related Commands

Command	Description
show mux	Displays general IP multiplexing information.

ipv4-address

To configure the IPv4 address for the Local Mobility Anchor (LMA) within MAG, for the Mobile Access Gateway (MAG) with LMA, or for the LMA or MAG within the Proxy Mobile IPv6 (PMIPv6) domain, use the **ipv4-address** command in the appropriate configuration mode. To remove the IPv4 address for the LMA or MAG, use the **no** form of this command.

ipv4-address *ipv4-address*

no ipv4-address

Syntax Description

ipv4-address	The IPv4 address for the LMA or MAG.

Command Default

No IPv4 address is configured for the LMA or MAG.

Command Modes

MAG-LMA configuration (config-ipv6-pmipv6mag-lma)

LMA-MAG configuration (config-ipv6-pmipv6lma-mag)

PMIPV6 domain LMA configuration (config-ipv6-pmipv6-domain-lma)

PMIPV6 domain MAG configuration (config-ipv6-pmipv6-domain-mag)

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.
Cisco IOS XE Release 3.6S	This command was modified. This command was made available in LMA-MAG configuration mode.
15.2(4)M	This command was integrated into Cisco IOS Release 15.2(4)M.

Usage Guidelines

Use the **ipv4-address** command in PMIPV6 domain LMA configuration mode to configure the IPv4 address for the LMA within the PMIPV6 domain.

Use the **ipv4-address** command in PMIPV6 domain MAG configuration mode to configure the IPv4 address for the MAG within the PMIPV6 domain.

Use the **ipv4-address** command in MAG-LMA configuration mode to configure the IPv4 address for the LMA within the MAG.

Use the **ipv4-address** command in LMA-MAG configuration mode to configure the IPv4 address for the MAG within the LMA.

Examples

The following example shows how to configure the IPv4 address for the LMA within the PMIPV6 domain:

```
Device(config)# ipv6 mobile pmipv6-domain dn1
Device(config-ipv6-pmipv6-domain)# lma lma1
Device(config-ipv6-pmipv6-domain-lma)# ipv4-address 10.1.1.1
```

The following example shows how to configure the IPv4 address for the MAG within the PMIPV6 domain:

```
Device(config)# ipv6 mobile pmipv6-domain dn1
Device(config-ipv6-pmipv6-domain)# mag mag1
Device(config-ipv6-pmipv6-domain-mag)# ipv4-address 10.1.2.1
```

The following example shows how to configure the IPv4 address for the LMA within the MAG:

```
Device(config)# ipv6 mobile pmipv6-domain dn1
Device(config-ipv6-pmipv6-domain)# exit
Device(config)# ipv6 mobile pmipv6-mag mag1 domain dn1
Device(config-ipv6-pmipv6-mag)# lma lma1 dn1
Device(config-ipv6-pmipv6mag-lma)# ipv4-address 10.1.2.1
```

The following example shows how to configure the IPv4 address for the MAG within the LMA:

```
Device(config)# ipv6 mobile pmipv6-domain dn1
Device(config-ipv6-pmipv6-domain)# exit
Device(config)# ipv6 mobile pmipv6-lma lma1 domain dn1
Device(config-ipv6-pmipv6-lma)# mag mag1 dn1
Device(config-ipv6-pmipv6lma-mag)# ipv4-address 10.1.2.1
```

Related Commands

Command	Description
ipv6 mobile pmipv6-domain	Configures the PMIPV6 domain.
ipv6 mobile pmipv6-mag	Configures the MAG for the PMIPV6 domain.
lma	Configures the LMA within the PMIPV6 domain.
mag	Configures the MAG within the PMIPV6 domain.

ipv6-address (proxy mobile ipv6)

To configure the IPv6 address for a Local Mobility Anchor (LMA) or a Mobile Access Gateway (MAG) within the Proxy Mobile IPv6 (PMIPv6) domain for an LMA within a MAG or for a MAG within an LMA, use the **ipv6-address** command in the appropriate configuration mode. To remove the IPv6 address for the LMA or MAG, use the **no** form of this command.

ipv6-address *ipv6-address*

no ipv6-address

Syntax Description

ipv6-address	The IPv6 address for the LMA or MAG.

Command Default

No IPv6 address is configured for the LMA or MAG.

Command Modes

MAG-LMA configuration (config-ipv6-pmipv6mag-lma)

LMA-MAG configuration (config-ipv6-pmipv6lma-mag)

PMIPV6 domain LMA configuration (config-ipv6-pmipv6-domain-lma)

PMIPV6 domain MAG configuration (config-ipv6-pmipv6-domain-mag)

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.
Cisco IOS XE Release 3.6S	This command was modified. This command was made available in LMA-MAG configuration mode.
15.2(4)M	This command was integrated into Cisco IOS Release 15.2(4)M.

Usage Guidelines

Use the **ipv6-address** command in PMIPV6 domain LMA configuration mode to configure the IPv6 address for the LMA within the PMIPV6 domain.

Use the **ipv6-address** command in PMIPV6 domain MAG configuration mode to configure the IPv6 address for the MAG within the PMIPV6 domain.

Use the **ipv6-address** command in MAG-LMA configuration mode to configure the IPv6 address for the LMA within the MAG.

Use the **ipv6-address** command in LMA-MAG configuration mode to configure the IPv6 address for the MAG within the LMA.

Examples

The following example shows how to configure an IPv6 address for an LMA within the PMIPV6 domain:

```
Router(config)# ipv6 mobile pmipv6-domain dn1
Router(config-ipv6-pmipv6-domain)# lma lma1
Router(config-ipv6-pmipv6-domain-lma)# ipv6-address 2001:0DB8:2:3::1
```

The following example shows how to configure an IPv6 address for a MAG within the PMIPV6 domain:

```
Router(config)# ipv6 mobile pmipv6-domain dn1
Router(config-ipv6-pmipv6-domain)# mag mag1
Router(config-ipv6-pmipv6-domain-mag)# ipv6-address 2001:0DB8:2:3::2
```

The following example shows how to configure an IPv6 address for a LMA within a MAG:

```
Router(config)# ipv6 mobile pmipv6-domain dn1
Router(config-ipv6-pmipv6-domain)# exit
Router(config)# ipv6 mobile pmipv6-mag mag1 domain dn1
Router(config-ipv6-pmipv6-mag)# lma lma1 dn1
Router(config-ipv6-pmipv6mag-lma)# ipv6-address 2001:0DB8:2:3::2
```

The following example shows how to configure an IPv6 address for a MAG within an LMA:

```
Router(config)# ipv6 mobile pmipv6-domain dn1
Router(config-ipv6-pmipv6-domain)# exit
Router(config)# ipv6 mobile pmipv6-lma lma1 domain dn1
Router(config-ipv6-pmipv6-lma)# mag mag1 dn1
Router(config-ipv6-pmipv6lma-mag)# ipv6-address 2001:0DB8:2:3::2
```

Related Commands

Command	Description
ipv6 mobile pmipv6-domain	Configures PMIPV6 domain.
ipv6 mobile pmipv6-lma	Configures LMA for PMIPv6 domain.
ipv6 mobile pmipv6-mag	Configures MAG for PMIPV6 domain.
lma	Configures LMA within PMIPV6 domain.
mag	Configures MAG within PMIPV6 domain.

ipv6 mobile pmipv6-domain

To configure the Proxy Mobile IPv6 (PMIPV6) domain, use the **ipv6 mobile pmipv6-domain** command in global configuration mode. To remove the PMIPV6 domain configuration, use the **no** form of this command.

ipv6 mobile pmipv6-domain *domain-name* **[load-aaa]**

no ipv6 mobile pmipv6-domain *domain-name* **[load-aaa]**

Syntax Description

domain-name	PMIPV6 domain name.
load-aaa	(Optional) Loads the domain configuration from the authentication, authorization, and accounting (AAA) server.

Command Default

No PMIPV6 domain is configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.
15.2(4)M	This command was integrated into Cisco IOS Release 15.2(4)M

Usage Guidelines

Use the **ipv6 mobile pmipv6-domain** command to enter PMIPV6 domain configuration mode and configure the domain-specific parameters.

Use the **ipv6 mobile pmipv6-domain** *domain-name* **load-aaa** to create the PMIPV6 domain using the configuration from AAA.

Examples

The following example shows how to enter PMIPV6 domain configuration mode to configure the PMIPV6 domain:

```
Device(config)# ipv6 mobile pmipv6-domain dn1
Device(config-ipv6-pmipv6-domain)#
```

The following example shows how to load the domain configuration from the AAA server:

```
Device(config)# ipv6 mobile pmipv6-domain dn1 load-aaa
```

Related Commands

Command	Description
show interfaces tunnel	Displays PMIPV6 domain tunnel information.

ipv6 mobile pmipv6-lma

To enable Local Mobility Anchor (LMA) service on the router and to configure the Proxy Mobile IPv6 (PMIPv6) domain for the LMA, use the **ipv6 mobile pmipv6-lma** command in global configuration mode. To disable the LMA service, use the **no** form of this command.

ipv6 mobile pmipv6-lma *lma-id* **domain** *domain-name* **[force]**

no ipv6 mobile pmipv6-lma *lma-id* **domain** *domain-name*

Syntax Description

lma-id	LMA identifier. This can be an instance identifier or any string that uniquely identifies the LMA.
domain *domain-name*	Specifies the PMIP domain to which the LMA belongs.
force	(Optional) Resets all parameter values to the default values set in the PMIP domain.

Command Default

LMA service on the router is not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.6S	This command was introduced.

Usage Guidelines

Use the **ipv6 mobile pmipv6-lma** command to enable the LMA service on the router. This command configures LMA-specific parameter values to the default configuration available in the PMIP domain, and enters LMA configuration mode.

Use the **ipv6 mobile pmipv6-lma** *lma-id* **domain** *domain-name* **force** command to set the LMA-specific parameter values to the default values set in the PMIPv6 domain.

The MAG service depends on the network time protocol (NTP) service, the IPv4 or IPv6 routing, and the IPv4 or IPV6 address configuration on interfaces.

Examples

The following example shows how to configure the LMA:

```
Device(config)# ipv6 mobile pmipv6-lma lma1 domain dn1
Device(config-ipv6-pmipv6-lma)#
```

The following example shows how to reset the LMA configuration to the default configuration available in the PMIP domain:

```
Device(config)# ipv6 mobile pmipv6-lma lma1 domain dn1 force
```

Related Commands

Command	Description
ipv6 mobile pmipv6-domain	Configures the PMIP domain.
show ipv6 mobile pmipv6 lma globals	Displays the global LMA configuration.

ipv6 mobile pmipv6-mag

To enable the Mobile Access Gateway (MAG) service on the router and to configure the Proxy Mobile IPv6 (PMIP) domain for the MAG, use the **ipv6 mobile pmipv6-mag** command in global configuration mode. To disable the MAG service, use the **no** form of this command.

ipv6 mobile pmipv6-mag *mag-id* **domain** *domain-name* **[force]**

no ipv6 mobile pmipv6-mag *mag-id* **domain** *domain-name*

Syntax Description

mag-id	MAG identifier. This can be Network Access Identifier or any string that uniquely identifies the MAG.
domain *domain-name*	Specifies the PMIP domain to which the MAG belongs.
force	(Optional) Resets all parameter values to the default values set in the PMIP domain.

Command Default

MAG service on the router is not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.

Usage Guidelines

Use the **ipv6 mobile pmipv6-mag** *mag-id* **domain** *domain-name* command to enable the MAG service on the router. This command configures the MAG-specific parameter values to the default configuration available in the PMIP domain, and enters MAG configuration mode.

Use the **ipv6 mobile pmipv6-mag** *mag-id* **domain** *domain-name* **force** command to set the MAG-specific parameter values to the default values set in the PMIP domain.

The MAG service depends on the network time protocol service, IPv4/IPv6 routing, and IPv4/IPV6 address configuration on the interfaces.

Examples

The following example shows how to configure the MAG:

```
Router(config)# ipv6 mobile pmipv6-mag mag1 domain dn1
Router(config-ipv6-pmipv6-mag)#
```

The following example shows how to reset the MAG configuration to the default configuration available in the PMIP domain:

```
Router(config)# ipv6 mobile pmipv6-mag mag1 domain dn1 force
```

Related Commands

Command	Description
ipv6 mobile pmipv6-domain	Configures the PMIP domain.
show ipv6 mobile pmipv6 mag globals	Displays the global MAG configuration.

ipv6 mux

To enable IP multiplexing in IPv6 on an interface, use the **ipv6 mux** command in interface configuration mode. To disable IP multiplexing on an interface, use the **no** form of the command.

ipv6 mux

no ipv6 mux

Syntax Description

This command has no arguments or keywords.

Command Default

IP multiplexing is disabled on the interface.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.2(2)GC	This command was introduced.
15.2(4)M	This command was integrated into Cisco IOS Release 15.2(4)M.

Usage Guidelines

IP multiplexing must be enabled on the interface before the interface can receive or send IP multiplexing superframes.

Examples

The following example shows how to configure IP multiplexing in IPv6 on FastEthernet 0/1:

```
Router# configure terminal
Router(config)# interface fastethernet0/1
Router(config-if)# ipv6 address FE80::A8BB:CCFF:FE01:5700
Router(config-if)# ipv6 enable
Router(config-if)# ipv6 mux
Router(config-if)# exit
Router(config)#
```

Related Commands

Command	Description
show mux interface	Displays configured IP multiplexing statistics for an interface.

ipv6 mux cache

To set the IPv6 multiplexing cache size in bytes, use the **ipv6 mux cache** command in global configuration mode. To return to the default setting, use the **no** form of this command.

ipv6 mux cache *size*

no ipv6 mux cache *size*

Syntax Description

size	Maximum cache size in bytes. The range is 1,000,000 to 4,294,967,295.

Command Default

The default cache size is 1,000,000 bytes.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.2(2)GC	This command was introduced.
15.2(4)M	This command was integrated into Cisco IOS Release 15.2(4)M.

Usage Guidelines

If you do not enter a cache size, the IPv6 multiplexing packet handler defaults to 1,000,000 bytes. A 1,000,000 byte cache contains 11,363 entries.

Examples

The following example shows how to configure the IPv6 multiplexing cache size to 5,000,000:

```
Router# configure terminal
Router(config)# ipv6 mux cache 5000000
Router(config)#
```

Related Commands

Command	Description
show mux cache	Displays IP multiplexing cache statistics.

ipv6 mux policy

To create an IPv6 multiplexing differentiated services code point (DSCP) policy with a specified name, use the **ipv6 mux policy** command in global configuration mode. To delete the IPv6 multiplexing policy, use the **no** form of this command.

ipv6 mux policy *policy-name*

no ipv6 mux policy *policy-name*

Syntax Description

policy-name	Name of the IPv6 multiplexing policy.

Command Default

No policies are created.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.2(2)GC	This command was introduced.
15.2(4)M	This command was integrated into Cisco IOS Release 15.2(4)M.

Usage Guidelines

You can specify up to three policies in addition to the default policy.

If you do not configure an IPv6 multiplexing policy, all IPv6 multiplexing packets are sent using the default IPv6 multiplexing policy with a DSCP value equal to 0.

Examples

The following example shows how to configure an IPv6 multiplexing DSCP policy with the name *routeRTP-SJ* and enter IPv6 multiplexing policy configuration mode:

```
Router# configure terminal
Router(config)# ipv6 mux policy routeRTP-SJ
Router(config-ipmux-policy-v6)#
```

Related Commands

Command	Description
show mux profile	Displays multiplexing statistics and the configuration for a specific IP multiplexing profile.

ipv6 mux profile

To create an IPv6 multiplexing profile with a specified name, use the **ipv6 mux profile** command in global configuration mode. To delete the IPv6 multiplexing profile, use the **no** form of this command.

ipv6 mux profile *profile-name*

no ipv6 mux profile *profile-name*

Syntax Description

profile-name	Name of the IPv6 multiplexing profile.

Command Default

No default profile exists.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.2(2)GC	This command was introduced.
15.2(4)M	This command was integrated into Cisco IOS Release 15.2(4)M.

Usage Guidelines

You can specify up to 500 profiles.

Examples

The following example shows how to configure an IPv6 multiplexing profile with the name *routeRTP-SJ* and enter IPv6 multiplexing profile configuration mode:

```
Router# configure terminal
Router(config)# ipv6 mux profile routeRTP-SJ
Router(config-ipmux-profile-v6)#
```

Related Commands

Command	Description
show mux profile	Displays multiplexing statistics and the configuration for a specific IP multiplexing profile.

ipv6 mux udpport

To specify a destination UDP port to use for IPv6 multiplexed packets, use the **ipv6 mux udpport** command in global configuration mode. To return to the default setting, use the **no** form of this command.

ipv6 mux udpport *port-number*

no ipv6 mux udpport

Syntax Description

port-number	UDP port number. The range is 1,024 to 49,151.

Command Default

The default port number is 6,682.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.2(2)GC	This command was introduced.
15.2(4)M	This command was integrated into Cisco IOS Release 15.2(4)M.

Usage Guidelines

If you do not enter a port number, the system uses the default port 6,682.

Examples

The following example shows how to configure the UDP port for IP multiplexed packets to 5,000:

```
Router# configure terminal
Router(config)# ipv6 mux udpport 5000
Router(config)#
```

Related Commands

Command	Description
show mux	Displays general IP multiplexing information.

lma

To specify the Local Mobility Anchors (LMAs), or to configure the LMA for the mobile node (MN) or the Mobile Access Gateway (MAG), use the **lma** command in the appropriate configuration mode. To disable the LMA configuration, use the **no** form of this command.

lma *lma-id domain-name*

no lma *lma-id*

Syntax Description

lma-id	LMA identifier.
domain-name	Domain name to which the LMA belongs. This argument is only available in MAG configuration mode.

Command Default

The LMA within the PMIPV6 domain is not configured. The LMA for the MN within the PMIPV6 domain is not configured.

Command Modes

MAG configuration (config-ipv6-pmipv6-mag)

Mobile node configuration (config-ipv6-pmipv6-domain-mn)

PMIPV6 domain configuration (config-ipv6-pmipv6-domain)

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.
15.2(4)M	This command was integrated into Cisco IOS Release 15.2(4)M.

Usage Guidelines

Use the **lma** command in PMIPV6 domain configuration mode to enter LMA configuration mode and configure IPv4 and IPv6 addresses for the LMA within the PMIPV6 domain.

Use the **lma** command in MN configuration mode to specify the LMA for the MN within the PMIPV6 domain.

Use the **lma** command in MAG configuration mode to specify the LMA for the MAG.

Examples

The following example shows how to enter LMA configuration mode to configure the LMA in PMIPV6 domain configuration mode:

```
Router(config)# ipv6 mobile pmipv6-domain dn1
Router(config-ipv6-pmipv6-domain)# lma lma1
Router(config-ipv6-pmipv6-domain-lma)#
```

The following example shows how to configure the LMA for the MN within the PMIPV6 domain:

```
Router(config)# ipv6 mobile pmipv6-domain dn1
Router(config-ipv6-pmipv6-domain)# nai example@example.com
Router(config-ipv6-pmipv6-domain-mn)# lma lma1
```

The following example shows how to configure the LMA for the MAG within the PMIPV6 domain:

```
Router(config)# ipv6 mobile pmipv6-mag mag1 domain dn1
Router(config-ipv6-pmipv6-mag)# lma lma1 dn1
Router(config-ipv6-pmipv6mag-lma)#
```

Related Commands

Command	Description
ipv6 mobile pmipv6-domain	Configures the PMIPV6 domain.
nai	Configures the Network Access Identifier for the mobile node within a PMIPV6 domain.

local-routing-mag

To enable local routing for the Mobile Access Gateway (MAG), use the **local-routing-mag** command in PMIPv6 domain configuration mode or MAG configuration mode. To disable local routing for the MAG, use the **no** form of this command.

local-routing-mag

no local-routing-mag

Syntax Description

This command has no arguments or keywords.

Command Default

Local routing is not enabled for the MAG.

Command Modes

MAG configuration (config-ipv6-pmipv6-mag)

PMIP domain configuration (config-ipv6-pmipv6-domain)

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.
15.2(4)M	This command was integrated into Cisco IOS Release 15.2(4)M.

Examples

The following example shows how to enable local routing for the MAG in PMIPV6 configuration mode:

```
Router(config)# ipv6 mobile pmipv6-domain dn1
Router(config-ipv6-pmipv6-domain)# local-routing-mag
```

The following example shows how to enable local routing for the MAG in MAG configuration mode:

```
Router(config)# ipv6 mobile pmipv6-domain dn1
Router(config-ipv6-pmipv6-domain)# exit
Router(config)# ipv6 mobile pmipv6-mag mag1 domain dn1
Router(config-ipv6-pmipv6-mag)# local-routing-mag
```

Related Commands

Command	Description
ipv6 mobile pmipv6-domain	Configures the PMIPV6 domain.
ipv6 mobile pmipv6-mag	Configures the MAG for the PMIPV6 domain.

mag

To configure the Mobile Access Gateway (MAG) within the Proxy Mobile IPv6 (PMIPV6) domain or to configure the MAG within a Local Mobility Anchor (LMA), use the **mag** command in the PMIPV6 domain configuration mode or LMA configuration mode. To disable the MAG configuration, use the **no** form of this command.

mag *mag-id domain-id*

no mag *mag-id domain-id*

Syntax Description

mag-id	MAG identifier.
domain-id	PMIP domain identifier.

Command Default

The LMA within the PMIPV6 domain is not configured.

Command Modes

PMIPV6 domain configuration (config-ipv6-pmipv6-domain)

LMA configuration (config-ipv6-pmipv6-lma)

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.
Cisco IOS XE Release 3.6S	This command was modified. The *domain-id* argument was added.
15.2(4)M	This command was integrated into Cisco IOS Release 15.2(4)M.

Usage Guidelines

Use the **mag** command in PMIPV6 domain configuration mode to configure the MAG within the PMIPV6 domain.

Use the **mag** command in LMA configuration mode to specify the MAG for the LMA.

Examples

The following example shows how to configure the MAG in the PMIPV6 domain:

```
Device(config)# ipv6 mobile pmipv6-domain dn1
Device(config-ipv6-pmipv6-domain)# mag mag1
Device(config-ipv6-pmipv6-domain-mag)#
```

The following example shows how to configure the MAG for the LMA:

```
Device(config)# ipv6 mobile pmipv6-lma lmag1 domain dn1
```

```
Device(config-ipv6-pmipv6-lma)# mag mag1 dn1
Device(config-ipv6-pmipv6lma-mag)#
```

Related Commands

Command	Description
ipv6 mobile pmipv6-domain	Configures the PMIPV6 domain.

match access-list (PMIPv6)

To create a match clause and specify access lists, use the **match access-list** command in PMIPv6 domain mobile-map configuration mode. To remove the match clause and the access lists, use the **no** form of this command.

match access-list *acl-name*

no match access-list *acl-name*

Syntax Description

acl-name	Access list name.

Command Default

Match clause is not created.

Command Modes

PMIPv6 domain mobile map configuration (config-ipv6-pmipv6-domain-mobile-map)

Command History

Release	Modification
Cisco IOS XE Release 3.10S	This command was introduced.

Usage Guidelines

First create the extended named access list in the configuration mode. Mention the name of the access list in the **match access-list** command.

Examples

The following example shows how to configure the match access list for a mobile map:

```
Device(config)# ip access-list extended acl1
Device(config-ext-nacl)# permit icmp any any
Device(config-ext-nacl)# exit
Device(config)# ipv6 mobile pmipv6-domain dn1
Device(config-ipv6-pmipv6-domain)# mobile-map map1 10
Device(config-ipv6-pmipv6-domain-mobile-map)# match access-list acl1
```

Related Commands

Command	Description
ip access-list	define an IP access list or object-group ACL by name or number.
mobile-map	Configures a mobile map for the PMIPv6 domain.

matchdscp

To specify a differentiated services code point (DSCP) value used to match IP multiplexed packets for the policy, use the **matchdscp** command in IPv4 multiplexing policy configuration or IPv6 multiplexing policy configuration mode. To return to the default setting, use the **no** form of this command.

matchdscp *DSCP-value*

no matchdscp *DSCP-value*

Syntax Description

DSCP-value	

	DSCP value. The range is 0 to 63. The following DSCP values are also valid: • **af11** —Match packets with AF11 DSCP (001010) • **af12** —Match packets with AF12 DSCP (001100) • **af13** —Match packets with AF13 DSCP (001110) • **af21** —Match packets with AF21 DSCP (010010) • **af22** —Match packets with AF22 DSCP (010100) • **af23** —Match packets with AF23 DSCP (010110) • **af31** —Match packets with AF31 DSCP (011010) • **af32** —Match packets with AF32 DSCP (011100) • **af33** —Match packets with AF33 DSCP (011110) • **af41** —Match packets with AF41 DSCP (100010) • **af42** —Match packets with AF42 DSCP (100100) • **af43** —Match packets with AF43 DSCP (100110) • **cs1** —Match packets with CS1 (precedence 1) DSCP (001000) • **cs2** —Match packets with CS2 (precedence 2) DSCP (010000) • **cs3** —Match packets with CS3 (precedence 3) DSCP (011000) • **cs4** —Match packets with CS4 (precedence 4) DSCP (100000) • **cs5** —Match packets with CS5 (precedence 5) DSCP (101000) • **cs6** —Match packets with CS6 (precedence 6) DSCP (110000) • **cs7** —Match packets with CS7 (precedence 7) DSCP (111000)

	• **default** —Match packets with default DSCP (000000) • **ef** —Match packets with EF DSCP (101110)

Command Default

No DSCP values are set.

Command Modes

IP multiplexing policy configuration (config-ipmux-policy)

IPv6 multiplexing policy configuration (config-ipmux-policy-v6)

Command History

Release	Modification
15.2(2)GC	This command was introduced.
15.2(4)M	This command was integrated into Cisco IOS Release 15.2(4)M.

Usage Guidelines

Make sure that the DSCP values do not overlap between policies. If the DSCP values do overlap, then the first policy to match the DSCP value from the top of the list is selected.

You can enter more than one value.

Examples

The following example shows how to configure the DSCP value to 45 in the IPv6 multiplexing policy *routeRTP-SJ* :

```
Router# configure terminal
Router(config)# ipv6 mux policy routeRTP-SJ
Router(config-ipmux-policy-v6)# matchdscp 45
Router(config-ipmux-policy-v6)# exit
Router(config)#
```

Related Commands

Command	Description
ip mux policy	Creates an IPv4 multiplexing DSCP policy with a specified name.
ipv6 mux policy	Creates an IPv6 multiplexing DSCP policy with a specified name.
show mux	Displays general IP multiplexing information.

maxlength

To specify the largest packet size that a multiplexing profile can hold for multiplexing, use the **maxlength** command in IPv4 multiplexing profile configuration or IPv6 multiplexing profile configuration mode. To return to the default setting, use the **no** form of this command.

maxlength *bytes*

no maxlength

Syntax Description

bytes	Maximum packet size, in bytes. The range is 64 to 1472.

Command Default

The policy multiplexes any packet that fits into the superframe.

Command Modes

IP multiplexing profile configuration (config-ipmux-profile)

IPv6 multiplexing profile configuration (config-ipmux-profile-v6)

Command History

Release	Modification
15.2(2)GC	This command was introduced.
15.2(4)M	This command was integrated into Cisco IOS Release 15.2(4)M.

Usage Guidelines

If you do not specify a maximum packet size for multiplexing, the maximum packet size will default to the configured MTU size minus the length of the superframe header (28 bytes for IPv4 and 48 bytes for IPv6).

Examples

The following example shows how to configure the maximum packet size that can go into the IP multiplexing profile routeRTP-SJ to 1472 bytes:

```
Router# configure terminal
Router(config)# ipv6 mux profile routeRTP-SJ
Router(config-ipmux-profile-v6)# maxlength 1472
Router(config-ipmux-profile-v6)# exit
Router(config)#
```

Related Commands

Command	Description
ip mux profile	Creates an IPv4 multiplexing profile with a specified name.

Command	Description
ipv6 mux profile	Creates an IPv6 multiplexing profile with a specified name.
show mux profile	Displays multiplexing statistics and the configuration for a specific IP multiplexing profile.

mn-profile-load-aaa

To load the profile configuration from the authentication, authorization, and accounting (AAA) server to the mobile node (MN), use the **mn-profile-load-aaa** command in PMIPV6 domain configuration mode. To disable triggering of AAA requests, use the **no** form of this command.

mn-profile-load-aaa

no mn-profile-load-aaa

Syntax Description

This command has no arguments or keywords.

Command Default

The profile configuration for the MN is not loaded.

Command Modes

PMIPV6 domain configuration (config-ipv6-pmipv6-domain)

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.
15.2(4)M	This command was integrated into Cisco IOS Release 15.2(4)M.

Usage Guidelines

Use the **mn-profile-load-aaa** command to configure the MN by using the configuration from the AAA server.

Examples

The following example shows how to configure the MN within the PMIPV6 domain by using the configuration from AAA:

```
Device(config)# ipv6 mobile pmipv6-domain dn1
Device(config-ipv6-pmipv6-domain)# mn-profile-load-aaa
```

Related Commands

Command	Description
ipv6 mobile pmipv6-domain	Configures the PMIPV6 domain.

mobile-map (LMA)

To apply a mobile map for an LMA, use the **mobile-map** command in the LMA configuration mode. To remove the mobile map, use the **no** form of this command.

mobile-map *map-name*

no mobile-map *map-name*

Syntax Description

map-name	Name of the mobile map.

Command Default

No mobile maps are applied.

Command Modes

LMA configuration (config-ipv6-pmipv6-lma)

Command History

Release	Modification
Cisco IOS XE Release 3.10S	This command was introduced.

Usage Guidelines

Use the **mobile-map** command to apply the mobile map that is configured in the PMIPv6 domain.

Examples

The following example shows how to apply a mobile map for an LMA:

```
Device(config)# ipv6 mobile pmipv6-lma lma1 domain d1
Device(config-ipv6-pmipv6-lma)# mobile-map map1
```

mobile-network (mobile router)

To specify the mobile router interface that is connected to the dynamic mobile network, use the **mobile-network** command in mobile router configuration mode. To disassociate the networks from the mobile router, use the **no** form of this command.

mobile-network *interface*

no mobile-network *interface*

Syntax Description

interface	Mobile router interface that is connected to the dynamic network.

Command Default

No default behavior or values.

Command Modes

Mobile router configuration

Command History

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

Usage Guidelines

The IP address and mask of the interface are added to the registration request to notify the home agent of the mobile networks. Once the home agent acknowledges the mobile network, the mobile router will no longer add the mobile network information in subsequent requests.

Examples

The following example shows how to enable mobile router services. In this example, the mobile router located at 10.0.0.3 is dynamically registering the primary interface address on Ethernet interface 3/2:

```
router mobile
ip mobile router
 address 10.0.0.3 255.0.0.0
 home-agent 10.0.0.4
 !specifies the Mobile Router interface connected to the mobile network
 mobile-network Ethernet3/2
 register lifetime 120
```

Related Commands

Command	Description
register (mobile networks)	Dynamically registers the mobile networks with the home agent.

mobile-network (PMIPv6)

To specify mobile address pools, from which a mobile network prefix is allocated to a logical mobile node (LMN), in a Local Mobility Anchor (LMA), use the **mobile-network pool** command in LMA-network configuration mode. To disassociate a mobile-network pool from an LMA, use the **no** form of this command.

mobile-network pool *address* **pool-prefix** *pool-prefix* **network-prefix** *network-prefix*

no mobile-network pool *address* **pool-prefix** *pool-prefix* **network-prefix** *network-prefix*

Syntax Description

pool *address*	IPv4 starting address in the mobile-network pool.
pool-prefix *pool-prefix*	Specifies the prefix length of the pool address.
network-prefix *network-prefix*	Specifies the prefix length of the mobile network address.

Command Default

No mobile network pool is specified in the LMA for the logical MN.

Command Modes

LMA-network configuration (config-ipv6-pmipv6lma-network)

Command History

Release	Modification
Cisco IOS XE Release 3.10S	This command was introduced.

Examples

The following example shows how to specify the name of the IPv4 address pool in an LMA:

```
Device(config)# ipv6 mobile pmipv6-lma lma1 domain dn1
Device(config-ipv6-pmipv6-lma)# network network1
Device(config-ipv6-pmipv6lma-network)# mobile-network pool 20.20.2.1 pool-prefix 24
network-prefix 30
```

Related Commands

Command	Description
ipv6 mobile pmipv6-domain	Configures the PMIPV6 domain.
nai	Configures the NAI for the MN within the PMIPV6 domain.

mode bypass

To enable Virtual Multipoint Interfaces (VMI) to support multicast traffic, use the **mode bypass** command in interface configuration mode. To return the interface to the default mode of aggregate, use the **no** form of this command.

mode [**aggregate**| **bypass**]

no mode bypass

Syntax Description

aggregate	Sets the mode to aggregate. All virtual-access interfaces created by PPPoE sessions are logically aggregated under the VMI.
bypass	Sets the mode to bypass.

Command Default

No mode

Command Modes

Interface configuration

Command History

Release	Modification
12.4(15)XF	This command was introduced.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T to support multicast traffic on Virtual Multipoint Interfaces (VMIs).

Usage Guidelines

Use the mode bypass command when you need to support multicast traffic in router-to-radio configurations.

Aggregate Mode

The default mode for operation of the VMI is **aggregate** mode. In aggregate mode, all of the virtual-access interfaces created by PPPoE sessions are logically aggregated under the VMI. As such, applications above Layer 2, such as, EIGRP and OSPFv3, should be defined on the VMI interface only. Packets sent to the VMI will be correctly forwarded to the correct virtual-access interface.

Bypass Mode

Using **bypass** mode is recommended for multicast applications.

In **bypass** mode, the virtual-access interfaces are directly exposed to applications running above Layer2. In bypass mode, definition of a VMI is still required because the VMI will continue to manage presentation of cross-layer signals, such as, neighbor up, neighbor down, and metrics. However, applications will still be aware on the actual underlying virtual-access interfaces and send packets to them directly.

Using **bypass** mode can cause databases in the applications to be larger because knowledge of more interfaces are required for normal operation.

After you enter the **mode bypass** command, Cisco recommends that you copy the running configuration to NVRAM. because the default mode of operation for VMI is to logically aggregate the virtual-access interfaces.

Examples

The following example sets the interface mode to bypass:

```
Router# enable
Router# configure terminal
Router(config)# interface vmi1
Router(config-if)# mode bypass
```

Related Commands

Command	Description
interface vmi	Creates a VMI interface.

mtu (IP multiplexing)

To specify the maximum transmission unit (MTU) size of an outbound superframe, use the **mtu** command in IP v4 multiplexing profile configuration or IPv6 multiplexing profile configuration mode. To return to the default setting, use the **no** form of this command.

mtu *bytes*

no mtu

Syntax Description

bytes	MTU size of the outbound superframe, in bytes. The range is 256 to 1,500.

Command Default

The maximum superframe packet size is 1,500 bytes.

Command Modes

IP multiplexing profile configuration (config-ipmux-profile)

IPv6 multiplexing profile configuration (config-ipmux-profile-v6)

Command History

Release	Modification
15.2(2)GC	This command was introduced.
15.2(4)M	This command was integrated into Cisco IOS Release 15.2(4)M.

Usage Guidelines

If you do not specify an MTU size, the IP multiplexing packet handler uses the default value of 1,500 bytes.

For each new packet being added to the superframe, the IP multiplexing packet handler checks the byte count of the multiplexing queue. If the queue byte count and the superframe header length exceed the configured MTU size, the software builds a superframe from the previous packets and the new packet becomes the first packet of the next superframe.

After you specify the MTU size, if you enter the **mtu** command again, the MTU size overwrites the previously entered size.

The superframe size specified in the **mtu** command includes the IP frame header for the superframe of 48 bytes for IPv6 and 28 bytes for IPv4 packets. Therefore an IPv6 MTU configured to 1,400 bytes will accept 1,352 bytes of data before sending a full superframe. An IPv4 MTU configured to 1,400 bytes will accept 1,372 bytes of data before sending a full superframe.

Examples

The following example shows how to configure the MTU size for IP multiplexing profile routeRTP-SJ to 1,000 bytes:

```
Router# configure terminal
Router(config)# ipv6 mux profile routeRTP-SJ
Router(config-ipmux-profile-v6)# mtu 1000
Router(config-ipmux-profile-v6)# exit
Router(config)#
```

Related Commands

Command	Description
ip mux profile	Creates an IPv4 multiplexing profile with a specified name.
ipv6 mux profile	Creates an IPv6 multiplexing profile with a specified name.
show mux profile	Displays multiplexing statistics and the configuration for a specific IP multiplexing profile.

multi-homed

To enable the multihoming feature for the mobile node (MN), use the **multi-homed** command in the PMIPV6 domain mobile node configuration mode. To remove the multihoming feature for the MN, use the **no** form of this command.

multi-homed

no multi-homed

Syntax Description

This command has no arguments or keywords.

Command Default

Multihoming is not enabled for the MN.

Command Modes

PMIPV6 domain mobile node configuration (config-ipv6-pmipv6-domain-mn)

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.
15.2(4)M	This command was integrated into Cisco IOS Release 15.2(4)M.

Examples

The following example shows how to enable multihoming for the MN:

```
Device(config)# ipv6 mobile pmipv6-domain dn1
Device(config-ipv6-pmipv6-domain)# nai example@example.com
Device(config-ipv6-pmipv6-domain-mn)# multi-homed
```

Related Commands

Command	Description
ipv6 mobile pmipv6-domain	Configures the PMIPV6 domain.
nai	Configures the Network Access Identifier for the MN within the PMIPV6 domain.

multi-path (mobile networks)

To override the global default setting and enable the home agent to process requests with multiple path support for a specific mobile router, use the **multi-path** command in mobile networks configuration mode. To disable this functionality, use the **no** form of this command.

multi-path [**metric** {**bandwidth**| **hopcount**}]

no multi-path [**metric** {**bandwidth**| **hopcount**}]

Syntax Description

metric	(Optional) Metric for multipath load balancing.
bandwidth	(Optional) Specifies that bandwidth is used as the metric. Bandwidth is the default metric.
hopcount	(Optional) Specifies that hop count is used as the metric.

Command Default

Multiple path support is disabled on the home agent.

Command Modes

Mobile networks configuration

Command History

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

Usage Guidelines

Multiple path support is enabled by default on the mobile router but is disabled by default on the home agent.

Examples

The following example shows how to configure the home agent to disable multiple path support for a specific mobile router:

```
!
ip mobile mobile-networks 10.1.1.14
 no multi-path
```

Related Commands

Command	Description
ip mobile home-agent multi-path	Enables the home agent to process registration requests with multiple path support for all mobile routers.

Command	Description
multi-path (mobile router)	Enables the mobile router to request multiple path support.

multi-path (mobile router)

To enable the mobile router to request multiple path support, use the **multi-path** command in mobile router configuration mode. To disable this functionality, use the **no** form of this command.

multi-path [**metric** {**bandwidth**| **hopcount**}]

no multi-path [**metric** {**bandwidth**| **hopcount**}]

Syntax Description

metric	(Optional) Metric for multipath load balancing.
bandwidth	Specifies that bandwidth is used as the metric. Bandwidth is the default metric.
hopcount	Specifies that hop count is used as the metric.

Command Default

Multiple path support is enabled on the mobile router.

Command Modes

Mobile router configuration.

Command History

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

Usage Guidelines

Multiple path support is enabled by default on the mobile router but disabled by default on the home agent.

Examples

The following example shows how to configure the mobile router to request multiple path support:

```
!
ip mobile router
 multi-path
```

Related Commands

Command	Description
ip mobile home-agent multi-path	Enables the home agent to process registration requests with multiple path support for all mobile routers.

Command	Description
multi-path (mobile networks)	Overrides the global default setting and enables the home agent to process requests with multiple path support for a specific mobile router.

multipath

To enable multipath support in Local Mobility Anchor (LMA), use the **multipath** command in LMA configuration mode. To remove the multipath support, use the no form of this command. To remove the multipath support, use the **no** form of this command.

multipath

no multipath

Syntax Description

There are no arguments and keywords.

Command Default

Multipath support is not enabled.

Command Modes

LMA configuration (config-ipv6-pmipv6-lma)

Command History

Release	Modification
Cisco IOS XE Release 3.10S	This command was introduced.

Examples

The following example shows how to enable multipath for LMA:

```
Device(config)# ipv6 mobile pmipv6-lma lma1 domain d1
Device(config-ipv6-pmipv6-lma)# multipath
```