Cisco IOS IP Mobility Command Reference

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

CONTENTS

aaa authorization ipmobile through ip mobile host

aaa authorization ipmobile

To authorize Mobile IP to retrieve security associations from the AAA server using TACACS+ or RADIUS, use the **aaa authorization ipmobile** command in global configuration mode. To remove authorization, use the **no** form of this command.

aaa authorization ipmobile {[**radius**| **tacacs**+]| **default**} [**group** *server-groupname*]

no aaa authorization ipmobile {[**radius**| **tacacs**+]| **default**} [**group** *server-groupname*]

Syntax Description

radius	Authorization list named radius.
tacacs+	Authorization list named tacacs+.
default	Default authorization list.
group *server-groupname*	(Optional) Name of the server group to use.

Command Default

AAA is not used to retrieve security associations for authentication.

Command Modes

Global configuration

Command History

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

Usage Guidelines

Mobile IP requires security associations for registration authentication. The security associations are configured on the router or on a AAA server. This command is not needed for the former; but in the latter case, this command authorizes Mobile IP to retrieve the security associations from the AAA server.

Once the authorization list is named, it can be used in other areas such as login. You can only use one named authorization list; multiple named authorization lists are not supported.

The **aaa authorization ipmobile default group** *server-groupname*command is the most commonly used method to retrieve security associations from the AAA server.

Note The AAA server does not authenticate the user. It stores the security association that is retrieved by the router to authenticate registration.

Examples

The following example uses TACACS+ to retrieve security associations from the AAA server:

```
aaa new-model
aaa authorization ipmobile tacacs+
tacacs-server host 1.2.3.4
tacacs-server key mykey
ip mobile host 10.0.0.1 10.0.0.5 virtual-network 10.0.0.0 255.0.0.0 aaa
```

The following example uses RADIUS as the default group to retrieve security associations from the AAA server:

```
aaa new-model
aaa authentication login default enable
aaa authorization ipmobile default group radius
aaa session-id common
radius-server host 128.107.162.173 auth-port 1645 acct-port 1646
radius-server retransmit 3
radius-server key cisco
ip mobile host 10.0.0.1 10.0.0.5 virtual-network 10.0.0.0 255.0.0.0 aaa
```

Related Commands

Command	Description
aaa new-model	Enables the AAA access control model.
ip mobile host	Configures the mobile host or mobile node group.
radius-server host	Specifies a RADIUS server host.
radius-server key	Sets the authentication and encryption key for all RADIUS communications between the router and the RADIUS daemon.
show ip mobile host	Displays mobile node information.
tacacs-server host	Specifies a TACACS host.
tacacs-server key	Sets the authentication encryption key used for all TACACS+ communications between the access server and the TACACS+ daemon.

access-list (IP multiplexing)

To assign an existing access list to an IP multiplexing profile, use the **access-list** command in IPv4 multiplexing profile configuration or IPv6 multiplexing profile configuration mode. To clear the access list associated with an IP multiplexing profile, use the **no** form of this command.

access-list {*standard-access-list-number*| *extended-access-list-number*| *name*}

no access-list

Syntax Description

standard-access-list-number	Standard access list number to use with the IP multiplexing profile. The range is 1 to 199.
extended-access-list-number	Extended access list number to use with the IP multiplexing profile. The range is 1300 to 2699.
name	Access list name to use with the IP multiplexing profile.

Command Default

No access list is configured.

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

You must configure an access list for IP multiplexing to work. The access list identifies the traffic to be considered for multiplexing. If you do not configure an access list, no packets are queued for multiplexing.

After the access list is created, if you enter the **access-list** command again, the new access list overwrites the previously entered access list. You must enter the **shutdown** and **no shutdown** commands to make the new access list take effect.

Create an access control ist (ACL) list by using the **ip access-list** or **ipv6 access-list** command. When you configure an ACL to use with IP multiplexing, filter only traffic based on the destination address, destination port, and protocol type. If you configure an ACL with other filter characteristics, unexpected or undesirable multiplexing decisions might occur. If you change an ACL associated with an IP multiplexing profile, you are prompted to enter the **shutdown** and **no shutdown** commands before the new access-list filters take effect.

If you delete an ACL from the profile, IP multiplexing will not send superframes; however, it still accepts superframes.

Examples

The following example shows how to configure the ACL routeRTP-SJ as the active ACL to filter packets for IP multiplexing:

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

Related Commands

Command	Description
ip access-list	Defines an IP access list or object-group ACL by name or number.
ipv6 access-list	Defines an IPv6 access list.
shutdown	Deactivates an IP multiplexing profile.

address (mobile router)

To set the home IP address of the mobile router, use the **address**commandinmobile router configuration mode. To remove the address, use the **no** form of this command.

address *address mask*

no address *address mask*

Syntax Description

address	Home IP address.
mask	Mask for the associated subnet.

Command Default

No default behavior or values.

Command Modes

Mobile router configuration

Command History

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

Usage Guidelines

The **address** command con figures the home IP address and subnet mask of the mobile router. The address and subnet mask identify the home network of the mobile router and are used to discover when the mobile router is at home.

Examples

The following example sets the home IP address and subnet mask of the mobile router:

```
ip mobile router
 address 10.1.0.1 255.255.0.0
```

Related Commands

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

address (proxy mobile IPv6)

To configure an IPv4, an IPv6, or dynamic address for a Mobile Access Gateway (MAG) or to configure an IPv4 or an IPv6 address on a Local Mobility Anchor (LMA), use the **address** command in MAG configuration mode or LMA configuration mode. To remove the IP address, use the **no** form of this command.

address {**ipv4** *ipv4-address*| **ipv6** *ipv6-address*| **dynamic**}

no address {**ipv4** *ipv4-address*| **ipv6** *ipv6-address*| **dynamic**}

Syntax Description

ipv4 *ipv4-address*	Specifies an IPv4 address for a MAG or an LMA.
ipv6 *ipv6-address*	Specifies an IPv6 address for a MAG or an LMA.
dynamic	Specifies a dynamic IP v4 address for a MAG.

Command Default

No IPv4 address or IPv6 address is configured for the MAG or the LMA.

Command Modes

MAG configuration (config-ipv6-pmipv6-mag)

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. This command was made available in LMA configuration mode.
15.2(4)M	This command was integrated into Cisco IOS Release 15.2(4)M.
Cisco IOS 15.4(1)T	This command was modified. The **dynamic** keyword was added..

Usage Guidelines

Use this command in MAG configuration mode to configure an IPv4 or IPv6 address or a dynamic IPv4 address for a MAG. Use this command in LMA configuration mode to configure an IPv4 or IPv6 address for an LMA.

The MAG or the LMA can have only one IPv4 address and one IPv6 address.

Examples

The following example shows how to configure an IPv6 address for 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)# address ipv6 2001:0DB8:2:5::1
```

The following example shows how to configure an IPv6 address for 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)# address ipv6 2001:0DB8:2:5::1
```

Related Commands

Command	Description
ipv6 mobile pmipv6-domain	Configures the PMIPv6 domain.
ipv6 mobile pmipv6-lma	Configures the LMA for a PMIPv6 domain.
ipv6 mobile pmipv6-mag	Configures the MAG for a PMIPv6 domain.

apn (proxy mobile IPv6)

To specify an access point name (APN) to the subscriber of the mobile node (MN) or for the Mobile Access Gateway (MAG) within the Proxy Mobile IPv6 (PMIPv6) domain, use the **apn** command in mobile node confguration mode or MAG configuration mode. To remove the APN specification, use the **no** form of this command.

apn *apn-name*

no apn

Syntax Description

apn-name	APN identifier.

Command Default

No APN is specified.

Command Modes

MAG configuration (config-ipv6-pmipv6-mag)

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 specify the APN for the MN within the PMIPv6 domain:

```
Device(config)# ipv6 mobile pmipv6-domain dn1
Device(config-ipv6-pmipv6-domain)# nai example@abc.com
Device(config-ipv6-pmipv6-domain-mn)# apn apn1
```

The following example shows how to specify the APN for the MAG within the PMIPv6 domain:

```
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)# apn apn1
```

Related Commands

Command	Description
ipv6 mobile pmipv6-domain	Configures the PMIPv6 domain.
ipv6 mobile pmipv6-mag	Configures MAG for the PMIPv6 domain.

Command	Description
nai	Configures the Network Access Identifier for the MN within the PMIPv6 domain.

auth-option

To enable authentication for the Proxy Mobile IPv6 (PMIP6) domain, the Local Mobility Anchor (LMA) peer entity within the Mobile Access Gateway (MAG), or the MAG peer entity within the LMA, use the **auth-option** command in the appropriate configuration mode. To disable the authentication, use the **no** form of this command.

auth-option spi {*spi-hex-value*| **decimal** *spi-decimal-value*} **key** {**ascii**| **hex**} *string*

no auth-option

Syntax Description

spi *spi-hex-value*	Specifies the Security Parameter Index (SPI) in hexadecimal format. The range is from 64 to FFFFFFFF.
decimal *spi-decimal-value*	Specifies the SPI value in decimal format. The range is from 256 to 12345678.
key	Specifies the security key.
ascii	Specifies the security key in ASCII format.
hex	Specifies the security key in hexadecimal format.
string	String key value.

Command Default

No authentication is set.

Command Modes

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

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

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

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 **auth-option** command in PMIPv6 configuration mode to configure the SPI and the key value for the PMIPV6 domain. The LMAs and the MAGs within the PMIPV6 domain use this configuration as the default.

Use the **auth-option** command in MAG-LMA configuration mode to configure the authentication for the LMA within the MAG.

Use the **auth-option** command in LMA-MAG configuration mode to configure the authentication for the MAG within the LMA.

Examples

The following example shows how to configure authentication for the PMIPV6 domain in PMIPV6 configuration mode, with the SPI in hexadecimal format and an ASCII string key value:

```
Device(config)# ipv6 mobile pmipv6-domain dn1
Device(config-ipv6-pmipv6-domain)# auth-option spi 67 key ascii key1
```

The following example shows how to configure the authentication for the LMA within the MAG in MAG-LMA configuration mode, with the SPI in decimal format and a string key value:

```
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)# auth-option spi decimal 258 key hex FFFF
```

The following example shows how to configure the authentication for the MAG peer entity within the LMA in LMA-MAG configuration mode, with the SPI in decimal format and a string key value:

```
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)# auth-option spi decimal 258 key hex FFFF
```

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 for the PMIPV6 domain.
mag	Configures the MAG for the PMIPV6 domain.

binding (proxy mobile IPv6)

To configure the binding update parameters for the Mobile Access Gateway (MAG), use the **binding** command in MAG configuration mode. To remove the configured binding update parameters, use the **no** form of this command.

binding {{**init-retx-time| max-retx-time**} *milliseconds*| {**lifetime| refresh-time**} *seconds*| **maximum** *number*}

no binding {**init-retx-time| max-retx-time| lifetime| refresh-time| maximum**}

Syntax Description

init-retx-time *milliseconds*	Specifies the initial timeout, in milliseconds (ms), between the Proxy Binding Updates (PBUs) and the Proxy Binding Acknowledgment (PBA) until the PBA is received. The range is from 100 to 65535. The default is 1.
lifetime *seconds*	Specifies the maximum lifetime, in seconds, permitted for the binding update entry. The range is from 10 to 65535. The default is 65535.
max-retx-time *milliseconds*	Specifies the maximum timeout in ms, between the PBUs and the PBAs until the PBA is received. The range is from 100 to 65535. The default is 32.
maximum *number*	Specifies the maximum number of binding update entries allowed. The range is from 1 to 40000.
refresh-time *seconds*	Specifies the binding update entry refresh time in seconds. The range is from 4 to 65535, and in multiples of 4. If the value entered is not a multiple of 4, the value configured may be rounded to the nearest lowest multiple of 4. The default is 300.

Command Default

Binding update parameters for the MAG is not configured.

Command Modes

MAG configuration (config-ipv6-pmipv6-mag)

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

The value for the **init-retx-time** keyword should be less than that for the **max-retx-time** keyword.

Examples

The following example shows how to configure binding update parameters for 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)# binding init-retx-time 110
Device(config-ipv6-pmipv6-mag)# binding max-retx-time 4000
Device(config-ipv6-pmipv6-mag)# binding lifetime 5000
Device(config-ipv6-pmipv6-mag)# binding maximum 200
Device(config-ipv6-pmipv6-mag)# binding refresh-time 2000
```

Related Commands

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

bce delete-wait-time

To specify the minimum time the Local Mobility Anchor (LMA) must wait, after receiving the delete notification from the Mobility Access Gateway (MAG), to delete the binding cache entries (BCEs) from the mobile node (MN), use the **bce delete-wait-time** command in LMA configuration mode. To restore the default value, use the **no** form of this command.

bce delete-wait-time *milliseconds*

no bce delete-wait-time*milliseconds*

Syntax Description

millisecond	Minimum time, in milliseconds, that the LMA waits before the BCE is deleted. • Range: 1 to 65535. Default: 10000.

Command Default

The time the LMA waits before it deletes the BCEs from the mobile node is 10000 ms.

Command Modes

LMA configuration (config-ipv6-pmipv6-lma)

Command History

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

Usage Guidelines

Use the **bce delete-wait-time** command to specify the minimum time in milliseconds the LMA must wait, after receiving the delete notification from the MAG, to delete a BCE.

To display the list of LMA bindings established over the Proxy Mobile IPv6 (PMIPv6) signaling plane, use the **show ipv6 mobile pmipv6 lma globals** command. The DeleteTime variable field displays the specified time the LMA should wait before it deletes BCEs.

Examples

The following example shows how to specify the minimum time the LMA must wait before deleting the BCEs.

```
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)# bce delete-wait-time 10
```

Related Commands

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

bce lifetime

To specify the lifetime of binding cache entries (BCEs) of a mobile node, use the **bce lifetime** command in LMA configuration mode. To restore to the default value, use the **no** form of this command.

bce lifetime *seconds*

no bce lifetime

Syntax Description

seconds	Lifetime of the BCEs. • The range is from 1 to 65535. The default is 3600.

Command Default

The lifetime of BCEs in the mobile node is 3600 seconds.

Command Modes

LMA configuration (config-ipv6-pmipv6-lma)

Command History

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

Usage Guidelines

Use the **bce lifetime** command to specify the lifetime of the BCEs of a mobile node.

To display the list of LMA bindings established over the Proxy Mobile IPv6 (PMIP) signaling plane, use the **show ipv6 mobile pmipv6 lma globals** command. The RegistrationLifeTime field displays the specified lifetime of the BCEs in the LMA.

Examples

The following example shows how to specify the lifetime of BCEs in 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)# bce lifetime 200
```

Related Commands

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

bce maximum

To specify the maximum number of binding cache entries (BCEs) that is allowed in a Local Mobility Anchor (LMA), use the **bce maximum** command in LMA configuration mode. To restore the default value, use the **no** form of this command.

bce maximum *maximum-number*

no bce maximum

Syntax Description

maximum-number	Maximum number of BCEs that is allowed in an LMA. • The range is from 1 to 128000. The default is 10000.

Command Default

The default number of BCEs that is allowed in an LMA is 10000.

Command Modes

LMA configuration (config-ipv6-pmipv6-lma)

Command History

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

Usage Guidelines

Use the **bce maximum** command in LMA configuration mode to specify the maximum number of binding cache entries (BCEs) that is allowed in an LMA.

To display the list of LMA bindings established over the Proxy Mobile IPv6 (PMIPv6) signaling plane, use the **show ipv6 mobile pmipv6 lma globals** command. The MaxBindings field displays the specified maximum number of BCEs allowed for the LMA.

Examples

The following example shows how to specify the maximum number of BCEs that is allowed in 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)#bce maximum 200
```

Related Commands

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

Command	Description
show ipv6 mobile pmipv6 lma globals	Displays the LMA global configuration details.

bri

To configure Binding Revocation Indication (BRI) message parameters, use the **bri** command in the appropriate configuration mode. To remove BRI message parameters, use the **no** form of this command.

Cisco IOS XE Release 3.4S

bri {**delay** {**max**| **min**} *milliseconds*| **retry** *number*}

no bri {**delay** {**max**| **min**}| **retry** *number*}

Cisco IOS XE Release 3.6S and Later Releases

bri {**delay** {**max**| **min**} *milliseconds*| **retries** *number*}

no bri {**delay** {**max**| **min**}| **retries** *number*}

Syntax Description

delay	Specifies the delay option.
max *milliseconds*	Specifies the maximum time, in milliseconds, for which the LMA or MAG should wait for the Binding Revocation Acknowledgment (BRA), from the MAG or LMA respectively, before retransmitting the BRI message. • The range is from 500 to 65536. The default is 2000.
min *milliseconds*	Specifies the minimum time, in milliseconds, for which the LMA or MAG should wait before transmitting the BRI message from MAG or LMA respectively. • The range is from 500 to 65536. The default is 100.
retries *number*	Specifies the maximum number of times the LMA should retransmit the BRI message until a BRA is received from MAG or LMA. • The range is from 1 to 10. The default is 1.

Command Default

BRI message parameters are not configured.

Command Modes

MAG configuration (config-ipv6-pmipv6-mag)

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. This command was made available in LMA configuration mode. The **retry** keyword was changed to **retries**.
15.2(4)M	This command was integrated into Cisco IOS Release 15.2(4)M

Usage Guidelines

Use the **bri** command in MAG configuration mode to configure BRI message parameters in the MAG.

Use the **bri** command in LMA configuration mode to configure BRI message parameters in the LMA.

The **max**, **min**, and **retries** keywords are represent the MAX_BRACK_TIMEOUT, InitMINDelayBRIs, and BRIMaxRetriesNumber variables described in RFC 5846.

Examples

The following example shows how to configure BRI retransmission parameters for 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)# bri delay max 4500
Device(config-ipv6-pmipv6-mag)# bri delay min 500
Device(config-ipv6-pmipv6-mag)# bri retries 6
```

The following example shows how to configure BRI retransmission parameters for 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)# bri delay max 4500
Device(config-ipv6-pmipv6-lma)# bri delay min 500
Device(config-ipv6-pmipv6-lma)# bri retries 6
```

Related Commands

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

clear ip mobile binding

To remove mobility bindings, use the **clear ip mobile binding**command in privileged EXEC mode.

clear ip mobile binding {**all** [**load** *standby-group-name*]| *ip-address* [**coa** *care-of-address*]| **nai** *string* [**session-id** *string*]| **vrf realm** *realm*} **[synch]**

Syntax Description

all	Clears all mobility bindings.
load *standby-group-name*	(Optional) Downloads mobility bindings for a standby group after a clear operation.
ip-address	IP address of a mobile node or mobile router.
coa *care-of-address*	(Optional) The binding corresponding to the IP address and its care-of address.
nai *string*	Network access identifier (NAI) of the mobile node.
session-id *string*	(Optional) Session identifier. The string value must be fewer than 25 characters in length.
vrf realm *realm*	Specifies the VRF realm.
synch	(Optional) Specifies that the bindings that are administratively cleared on the active home agent are synchronized to the standby home agent, and the bindings will be deleted on the standby home agent.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.1(3)T	The following keywords and argument were added: • **all** • **load** • *standby-group-name*
12.2(2)XC	The **nai** keyword was added.

Release	Modification
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.3(4)T	The *session-id* keyword was added.
12.4(9)T	The **coa** *care-of-address* keyword and argument combination were added.
12.4(11)T	The **vrf realm** *realm*and **synch** keywords and argument were added.

Usage Guidelines

The home agent creates a mobility binding for each roaming mobile node. Associated with the mobility binding is the tunnel to the visited network and a host route to forward packets destined for the mobile node. Typically, there should be no need to clear the binding because it expires after the lifetime is reached or when the mobile node deregisters.

When the mobility binding is removed through use of this command, the number of users on the tunnel is decremented and the host route is removed from the routing table. The mobile node is not notified.

If the **nai** *string* **session-id** *string* option is specified, only the binding entry with that session identifier is cleared. If the **session-id**keyword is not specified, all binding entries (potentially more than one, with different session identifiers) for that NAI are cleared. You can determine the **session-id** *string* value by using the **show ip mobile binding** command.

When the **synch** option is specified, bindings that are administratively cleared on the active home agent are synchronized to the standby home agent, and the bindings will be deleted on the standby home agent. When the redundancy mode is active-standby, the **synch** option will not take effect if the clear command is issued on the standby home agent.

Use this command with care, because it will disrupt any sessions used by the mobile node. After you use this command, the mobile node will need to reregister to continue roaming.

Examples

The following example administratively stops mobile node 192.168.100.10 from roaming:

```
Router# show ip mobile binding
Mobility Binding List:
Total 1
192.168.100.10:
    Care-of Addr 192.168.6.1, Src Addr 192.168.4.2,
    Lifetime granted 02:46:40 (10000), remaining 02:46:32
    Flags SbdmGvt, Identification B750FAC4.C28F56A8,
    Tunnel100 src 192.168.1.2 dest 192.168.6.1 reverse-allowed
    Routing Options - (G)GRE
Router# clear ip mobile binding 10.2.0.1
Router# show ip mobile binding
```

Related Commands

Command	Description
show ip mobile binding	Displays the mobility binding table.

clear ip mobile host-counters

To clear the mobility counters specific to each mobile node, use the **clear ip mobile host-counters**command in EXEC mode.

clear ip mobile host-counters [[*ip-address*| **nai** *string*] **undo**]

Syntax Description

ip-address	(Optional) IP address of a mobile node.
nai string	(Optional) Network access identifier of the mobile node.
undo	(Optional) Restores the previously cleared counters.

Command Modes

EXEC

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2(2)XC	The nai keyword was added.
12.2(13)T	The nai keyword was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines

This command clears the counters that are displayed when you use the show ip mobile host command. The **undo** keyword restores the counters (this option is useful for debugging).

Examples

The following example shows how the counters can be used for debugging:

```
Router# show ip mobile host
10.0.0.1:
    Allowed lifetime 10:00:00 (36000/default)
    Roaming status -registered-, Home link on virtual network 20.0.0.0/8
    Accepted 2, Last time 04/13/02 19:04:28
    Overall service time 00:04:42
    Denied 0, Last time -never-
    Last code ‘-never- (0)’
    Total violations 1
    Tunnel to MN - pkts 0, bytes 0
    Reverse tunnel from MN - pkts 0, bytes 0
    .
Router# clear ip mobile host-counters
Router# show ip mobile host-counters
20.0.0.1:
    Allowed lifetime 10:00:00 (36000/default)
    Roaming status -Unregistered-, Home link on virtual network 20.0.0.0/8
    Accepted 0, Last time -never-
    Overall service time -never-
    Denied 0, Last time -never-
    Last code ‘-never- (0)’
    Total violations 0
    Tunnel to MN - pkts 0, bytes 0
    Reverse tunnel from MN - pkts 0, bytes 0
```

Related Commands

Command	Description
show ip mobile host	Displays mobile node counters and information.

clear ip mobile router agent

To delete learned agents and the corresponding care-of address of the foreign agent from the mobile router agent table, use the **clear ip mobile router agent** command in privileged EXEC mode.

clear ip mobile router agent [*ip-address*]

Syntax Description

ip-address	(Optional) IP address of an agent. If not specified, all agents are deleted from the agent table.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

The mobile router maintains an agent table listing active agents and the corresponding care-of address of the foreign agent. The mobile router uses this agent table to decide which foreign agent to register with. The mobile router updates the table when it receives advertisements. If an advertisement expires, its entry is automatically deleted from the table.

The **clear ip mobile router agent** *ip-address*option allows you to remove a specific agent.

Examples

The following example removes all agents from the mobile router agent table:

```
Router# clear ip mobile router agent
```

Related Commands

Command	Description
show ip mobile router interface	Displays information about the agents for the mobile router.

clear ip mobile router registration

To delete registration entries from the mobile router registration table, use the **clear ip mobile router registration**command in privileged EXEC mode.

clear ip mobile router registration [*ip-address*]

Syntax Description

ip-address	(Optional) IP address of a specific agent. If not specified, all registration entries are deleted.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

The m obile router maintains a registration table listing registration entries that are used for retransmissions. For example, a registration request is sent when no reply is received or the lifetime is about to expire.

A registration request can be removed from the table to prevent further registration requests from being sent to the agent. The **clear ip mobile router registration** *ip-address*option allows you to remove a registration to a specific agent.

Clearing an active registration will cause the mobile router to attempt to deregister.

Examples

The following example removes all registration entries from the mobile router registration table:

```
Router# clear ip mobile router registration
```

Related Commands

Command	Description
show ip mobile router registration	Displays the pending and accepted registrations of the mobile router.

clear ip mobile router traffic

To clear the counters that the mobile router maintains, use the **clear ip mobile router traffic** command in privileged EXEC mode.

clear ip mobile router traffic

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

Mobile router counters are accumulated during operation. They are useful for debugging and monitoring.

Examples

The following example shows how the mobile router counters can be used for debugging:

```
Router# show ip mobile router traffic
Mobile Router Counters:
Agent Discovery:
  Solicitations sent 90, advertisements received 17
  Agent reboots detected 0
Registrations:
  Register 70, Deregister 0 requests sent
  Register 70, Deregister 0 replies received
  Requests accepted 68, denied 1 by HA 1 /FA 0
  Denied due to mismatched ID 1
  .
  .
  .
Router# clear ip mobile router traffic
Router# show ip mobile router traffic
Mobile Router Counters:
Agent Discovery:
  Solicitations sent 0, advertisements received 0
  Agent reboots detected 0
Registrations:
  Register 0, Deregister 0 requests sent
  Register 0, Deregister 0 replies received
  Requests accepted 0, denied 0 by HA 0 /FA 0
  Denied due to mismatched ID 0
  .
  .
  .
```

Related Commands

Command	Description
show ip mobile router traffic	Displays the counters that the mobile router maintains.

clear ip mobile secure

To clear and retrieve remote security associations, use the **clear ip mobile secure**commandinEXEC mode.

clear ip mobile secure {**host** *lower* **[upper]**| **nai** *string*| **empty**| **all**} **[load]**

Syntax Description

host	Mobile node host.
lower	IP address of mobile node. Can be used alone, or as lower end of a range of IP addresses.
upper	(Optional) Upper end of a range of IP addresses.
nai *string*	Network access identifier of the mobile node.
empty	Load in only mobile nodes without security associations. Must be used with the **load**keyword.
all	Clears all mobile nodes.
load	(Optional) Reload the security association from the AAA server after security association has been cleared.

Command Modes

EXEC

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2(2)XC	The nai keyword was added.
12.2(13)T	The nai keyword was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines

Security associations are required for registration authentication. They can be stored on an AAA server. During registration, they may be stored locally after retrieval from the AAA server. The security association on the router may become stale or out of date when the security association on the AAA server changes.

This command clears security associations that have been downloaded from the AAA server.

Note Security associations that are manually configured on the router or not stored on the router after retrieval from the AAA server are not applicable.

Examples

In the following example, the AAA server has the security association for user 10.2.0.1 after registration:

```
Router# show ip mobile secure host 10.2.0.1
Security Associations (algorithm,mode,replay protection,key):
10.2.0.1:
    SPI 300,  MD5, Prefix-suffix, Timestamp +/- 7,
    Key ‘oldkey’ 1230552d39b7c1751f86bae5205ec0c8
```

If you change the security association stored on the AAA server for this mobile node, the router clears the security association and reloads it from the AAA server:

```
Router# clear ip mobile secure host 10.2.0.1 load
Router# show ip mobile secure host 10.2.0.1
10.2.0.1:
    SPI 300,  MD5, Prefix-suffix, Timestamp +/- 7,
    Key ‘newkey’ 1230552d39b7c1751f86bae5205ec0c8
```

Related Commands

Command	Description
ip mobile secure	Specifies the mobility security associations for mobile host, visitor, home agent, and foreign agent.

clear ip mobile traffic

To clear counters, use the **clear ip mobile traffic**command inEXEC mode.

clear ip mobile traffic [undo]

Syntax Description

undo	(Optional) Restores the previously cleared counters.

Command Modes

EXEC

Command History

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

Usage Guidelines

Mobile IP counters are accumulated during operation. They are useful for debugging and monitoring.

This command clears all Mobile IP counters. The **undo** keyword restores the counters (which is useful for debugging). See the **show ip mobile traffic** command for a description of all counters.

Examples

The following example shows how counters can be used for debugging:

```
Router# show ip mobile traffic
IP Mobility traffic:
Advertisements:
    Solicitations received 0
    Advertisements sent 0, response to solicitation 0
Home Agent Registrations:
    Register 8, Deregister 0 requests
    Register 7, Deregister 0 replied
    Accepted 6, No simultaneous bindings 0
    Denied 1, Ignored 1
    Unspecified 0, Unknown HA 0
    Administrative prohibited 0, No resource 0
    Authentication failed MN 0, FA 0
    Bad identification 1, Bad request form 0
    .
Router# clear ip mobile traffic
Router# show ip mobile traffic
IP Mobility traffic:
Advertisements:
    Solicitations received 0
    Advertisements sent 0, response to solicitation 0
Home Agent Registrations:
    Register 0, Deregister 0 requests
    Register 0, Deregister 0 replied
    Accepted 0, No simultaneous bindings 0
    Denied 0, Ignored 0
    Unspecified 0, Unknown HA 0
    Administrative prohibited 0, No resource 0
```

```
Authentication failed MN 0, FA 0
Bad identification 0, Bad request form 0
```

Related Commands

Command	Description
show ip mobile traffic	Displays protocol counters.

clear ip mobile visitor

To remove visitor information, use the **clear ip mobile visitor**command inprivilegedEXEC mode.

clear ip mobile visitor [*ip-address*| **nai** *string* [**session-id** *string*] [*ip-address*]]

Syntax Description

ip-address	(Optional) IP address. If not specified, visitor information will be removed for all addresses.
nai string	(Optional) Network access identifier (NAI) of the mobile node.
session - id *string*	(Optional) Session identifier. The string value must be fewer than 25 characters in length.
ip-address	(Optional) IP address associated with the NAI.

Command Modes

EXEC

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2(2)XC	The nai keyword and associated variables were added.
12.2(13)T	The nai keyword and associated variables were integrated into Cisco IOS Release 12.2(13)T.
12.3(4)T	The **session-id** keyword was added.

Usage Guidelines

The foreign agent creates a visitor entry for each accepted visitor. The visitor entry allows the mobile node to receive packets while in a visited network. Associated with the visitor entry is the Address Resolution Protocol (ARP) entry for the visitor. There should be no need to clear the entry because it expires after lifetime is reached or when the mobile node deregisters.

When a visitor entry is removed, the number of users on the tunnel is decremented and the ARP entry is removed from the ARP cache. The visitor is not notified.

If the **nai** *string* **session-id** *string* option is specified, only the visitor entry with that session identifier is cleared. If the **session-id** keyword is not specified, all visitor entries (potentially more than one, with different session identifiers) for that NAI are cleared. You can determine the **session-id** *string* value by using the **show ip mobile visitor** command.

Use this command with care because it may terminate any sessions used by the mobile node. After you use this command, the visitor will need to reregister to continue roaming.

Examples

The following example administratively stops visitor 172.21.58.16 from visiting:

```
Router# clear ip mobile visitor 172.21.58.16
```

Related Commands

Command	Description
show ip mobile visitor	Displays the table containing the visitor list of the foreign agent.

clear ipv6 mobile pmipv6 lma

To reset the Proxy Mobile IPv6 (PMIPv6) domain Local Mobility Anchor (LMA) sessions, use the **clear ipv6 mobile pmipv6 lma** command in privileged EXEC mode.

clear ipv6 mobile pmipv6 lma *lma-name* {**binding** {**all**| **lma** *lma-v6-address*| **nai** *nai-string*}| **stats** [**domain** *domain-name* **peer** *peer-name*]}

Syntax Description

binding	Specifies the binding sessions.
all	Resets all sessions.
lma *lma-v6-address*	Resets the binding sessions for the LMA.
nai *nai-string*	Resets the binding sessions for the mobile node (MN).
stats	Specifies all LMA statistics.
domain *domain-name*	(Optional) Resets the statistics for the Mobile Access Gateway (MAG) in the PMIP domain.
peer *peer-name*	Specifies the MAG.

Command Default

No reset is initiated.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.6S	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 clear the binding sessions for the MN:

```
Device(config)# show ipv6 mobile pmipv6 lma lma1 binding
!
Total number of bindings: 1
----------------------------------------
[Binding][MN]: Domain: domain1, NAI: example@example.com
        [Binding][MN]: ATT: 3, LLID: aabb.cc00.c900
        [Binding][MN]: HOA: 192.0.2.7, Prefix: 24
        [Binding][MN]: HNP: DDDD::
```

```
        [Binding][MN][MAG]: Id: mag0
        [Binding][MN][MAG]: Lifetime: 3600(sec), Lifetime Remaining: 3500(sec)
        [Binding][MN][MAG]: Tunnel: Tunnel0
        [Binding][MN][MAG]: Default Router: 192.0.2.1
        [Binding][MN][GREKEY]: Upstream: 400, Downstream: 100

!
Device# clear ipv6 mobile pmipv6 lma lma1 binding nai example@example.com
Device# show ipv6 mobile pmipv6 lma bindings
!
Total number of bindings: 0
```

The following example shows how to clear all LMA statistics:

```
Device# clear ipv6 mobile pmipv6 lma stats
```

The following example shows how to clear LMA statistics for the MAG:

```
Device# clear ipv6 mobile pmipv6 lma stats domain D1 peer mag1
```

Related Commands

Command	Description
show ipv6 mobile pmipv6 lma bindings	Displays LMA bindings.
show ipv6 mobile pmipv6 lma globals	Displays the LMA configuration.
show ipv6 mobile pmipv6 lma stats	Displays LMA statistics.

clear ipv6 mobile pmipv6 mag

To reset the Proxy Mobile IPv6 (PMIPv6) domain Mobile Access Gateway (MAG) sessions, use the **clear ipv6 mobile pmipv6 mag** command in privileged EXEC mode.

Cisco IOS XE Release 3.4S

clear ipv6 mobile pmipv6 mag {**binding** {**all**| **lma** *lma-v6-address*| **nai** *nai-string* [**interface** *type number*]}| **stats** [**domain** *domain-name* **peer** *peer-name*]}

Cisco IOS Release 15.2(4)M

clear ipv6 mobile pmipv6 mag *mag-id* {**binding** {**all**| **lma** *lma-v6-address*| **nai** *nai-string* [**interface** *type number*]}| **stats** [**domain** *domain-name* **peer** *peer-name*]}

Syntax Description

mag-id	MAG identifier. This can be any string that uniquely identifies the MAG.
binding	Specifies the binding sessions.
all	Resets all sessions.
lma *lma-v6-address*	Resets the binding sessions for the Local Mobility Anchor (LMA).
nai *nai-string*	Resets the binding sessions for the mobile node (MN).
interface *type number*	(Optional) Resets the binding sessions for the MN interface.
stats	Specifies all MAG statistics.
domain *domain-name*	(Optional) Resets the statistics for the LMA in the PMIPV6 domain.
peer *peer-name*	(Optional) Specifies the LMA.

Command Default

PMIPV6 domain MAG sessions reset is not initiated.

Command Modes

Privileged EXEC (#)

Command History

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

Release	Modification
15.2(4)M	This command was modified. This command was integrated into Cisco IOS Release 15.2(4)M. The *mag-id* keyword was added.

Examples

The following example shows how to clear the binding sessions for the MN:

```
Device(config)# show ipv6 mobile pmipv6 mag mag1 bindings
!
Total number of bindings: 1
----------------------------------------
[Binding][MN]: Domain: D1, Nai: example3@example.com
        [Binding][MN]: State: ACTIVE
        [Binding][MN]: Interface: Ethernet0/0
        [Binding][MN]: Hoa: 0x11110106, att: 3, llid: aabb.cc00.ce00
        [Binding][MN][LMA]: Id: LMA2
        [Binding][MN][LMA]: lifetime: 3600
!
Device(config)# clear ipv6 mobile pmipv6 mag mag1 binding nai example3@example.com
Device(config)# show ipv6 mobile pmipv6 mag mag1 bindings
!
Total number of bindings: 0
```

The following example shows how to clear all MAG statistics:

```
Device(config)# clear ipv6 mobile pmipv6 mag mag1 stats
```

The following example shows how to clear MAG statistics for the LMA:

```
Device(config)# clear ipv6 mobile pmipv6 mag mag1 stats domain D1 peer lma1
```

Related Commands

Command	Description
show ipv6 mobile pmipv6 mag bindings	Displays MAG bindings.
show ipv6 mobile pmipv6 mag globals	Displays MAG configuration.
show ipv6 mobile pmipv6 mag stats	Displays MAG statistics.

clear mcsa statistics

To clear the mobile client service abstraction (MCSA) notification statistics, use the **clear mcsa statistics** command in privileged EXEC mode.

clear mcsa statistics {**sint**| **cint**}

Syntax Description

sint	Clears the service interface notification statistics.
cint	Clears the client interface notification statistics.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.8S	This command was introduced.

Examples

The following example shows how to clear the MCSA service interface notification statistics:

```
Device# clear mcsa statistics sint
```

Related Commands

Command	Description
show mcsa statistics	Displays the MCSA notification statistics.

collocated single-tunnel

To configure the number of tunnels between the mobile router and home agent when registering with a collocated care-of address (CCoA), use the **collocated single-tunnel**command in mobile router configuration mode.

collocated single-tunnel

Syntax Description

This command has no arguments or keywords.

Command Default

Defaults to single-tunnel enabled.

Command Modes

Mobile router

Command History

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

Usage Guidelines

This command is used as a “placeholder” only and defaults to single-tunnel enabled. This command can not be unconfigured. In future Cisco IOS releases, a dual-tunnel capability will be needed for IPSec between the mobile router and the home agent. At that time, this command will be optional with dual tunnels (**no collocated single-tunnel**) being the default. This command is provided now for backward compatibility when the dual-tunnel capablity is implemented.

debug ipv6 mobile lma

To enable debugging the Local Mobility Access (LMA) application programming interface (API), information, or events, use the **debug ipv6 mobile lma** command in privileged EXEC mode. To disable display of the debugging output, use the **no** form of this command.

debug ipv6 mobile lma {**api**| **events**| **info**}

no debug ipv6 mobile lma {**api**| **events**| **info**}

Syntax Description

api	Enables API-specific debug events.
events	Enables all events occurring within the LMA and the Mobile Access Gateway (MAG).
info	Provides debug information within the Proxy Mobile IPv6 (PMIP) module.

Command Default

Debugging is disabled.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.6S	This command was introduced.
15.2(4)M	This command was integrated into Cisco IOS Release 15.2(4)M.

Examples

The following sample output from the **debug ipv6 mobile lma api** command displays the APIs that are called during the call setup flow:

```
Device# debug ipv6 mobile lma api

*Mar 19 08:52:50.989: PMIPV6_LMA_API: pmipv6_lma_should_handle_pkt called
*Mar 19 08:52:50.989: MIP_PDL_API: pmipv6_pdl_get_timestamp API Called
*Mar 19 08:52:50.989: [PMIPV6_BINDING_API]: pmipv6_get_binding API called
*Mar 19 08:52:50.989: [PMIPV6_BINDING_API]: pmipv6_get_binding API called
*Mar 19 08:52:50.989: PMIPV6_LMA_API: pmipv6_lma_mn_do_state_transition called
*Mar 19 08:52:50.989: PMIPV6_LMA_API: lma_bce_state_transition called
*Mar 19 08:52:50.989: [PMIPV6_BINDING_API]: pmipv6_add_binding_entry API called
*Mar 19 08:52:50.989: [PMIPV6_BINDING_API]: pmipv6_get_binding API called
*Mar 19 08:52:50.989: PMIPV6_LMA_API: pmipv6_lma_mn_do_state_transition called
*Mar 19 08:52:50.989: PMIPV6_LMA_API: lma_bce_state_transition called
*Mar 19 08:52:50.989: MIP_PDL_API: mip_pdl_setupv4_tunnel API Called
*Mar 19 08:52:50.990: MIP_PDL_API: mip_pdl_get_handle_for_tunnel API Called
*Mar 19 08:52:50.990: MIP_PDL_API: mip_pdl_get_handle_for_tunnel API Called
```

```
*Mar 19 08:52:50.990: MIP_PDL_API: mip_pdl_setupv4_route API Called
*Mar 19 08:52:50.990: MIP_PDL_API: mip_pdl_get_handle_for_tunnel API Called
*Mar 19 08:52:50.990: MIP_PDL_API: mip_pdl_setupv6_route API Called
*Mar 19 08:52:50.990: [PMIPV6_BINDING_API]: pmipv6_update_binding_key API called
```

The following example shows the output of the **debug ipv6 mobile lma events** command:

```
Device# debug ipv6 mobile lma events

*Mar 20 12:08:54.703: PMIPV6_LMA_EVENT: Event (HI_UNKNOWN) received in
pmipv6_lma_mn_init_state_hndlr
*Mar 20 12:08:54.703: PMIPV6_LMA_EVENT: MN(name1@example.com) State Transition: MN_INIT ->
 MN_ACTIVE
*Mar 20 12:08:54.703: PMIPV6_LMA_EVENT: Event (HI_UNKNOWN) received in
pmipv6_lma_mn_active_state_entry
*Mar 20 12:08:54.703: PMIPV6_LMA_EVENT: BCE(name1@example.com) With ATT(4) State Transition:
 BCE_NULL -> BCE_INIT
*Mar 20 12:08:54.703: PMIPV6_LMA_EVENT: Event (HI_UNKNOWN) received in
pmipv6_lma_bce_init_state_entry
*Mar 20 12:08:54.703: PMIPV6_LMA_EVENT: Event (LMA_ADDRESS_ALLOC) received in
pmipv6_lma_mn_active_state_hndlr
*Mar 20 12:08:54.703: PMIPV6_LMA_EVENT: BCE(name1@example.com) With ATT(4) State Transition:
 BCE_INIT -> BCE_ACTIVE
*Mar 20 12:08:54.704: PMIPV6_LMA_EVENT: Event (LMA_ADDRESS_ALLOC) received in
pmipv6_lma_bce_active_state_entry
```

The following example shows the output of the **debug ipv6 mobile lma info** command:

```
Device# debug ipv6 mobile lma info

*Mar 20 12:10:11.975: [PMIPV6_PDB_INFO]:MN example1 found locally
*Mar 20 12:10:11.975: PMIPV6_LMA_INFO: Default (example1) profile set for this MN
*Mar 20 12:10:11.975: PMIPV6_LMA_INFO: PBU Received: MAG(mag2), MN(name1@example.com),
HI(4), Lifetime (3600), ATT (4), LLI(aabb.cc00.c901), HOA(0)
*Mar 20 12:10:11.975: [PMIPV6_BINDING_INFO_KEY]: Keytype as NAI. NAI: name1@example.com
*Mar 20 12:10:11.975: [PMIPV6_BINDING_INFO]: binding not found
*Mar 20 12:10:11.975: [PMIPV6_BINDING_INFO_KEY]: Keytype as NAI. NAI: name1@example.com
*Mar 20 12:10:11.975: [PMIPV6_BINDING_INFO]: binding not found
*Mar 20 12:10:11.975: PMIPV6_LMA_INFO: Network name(n1) taken from MN profile
*Mar 20 12:10:11.975: [PMIPV6_BINDING_INFO_KEY]: Keytype as NAI. NAI: name1@example.com
*Mar 20 12:10:11.975: [PMIPV6_BINDING_INFO]: binding added New NAI AVL node created
*Mar 20 12:10:11.975: PMIPV6_LMA_INFO: Added BCE(name1@example.com), with key(7) to Binding
 Module
*Mar 20 12:10:11.975: [PMIPV6_BINDING_INFO_KEY]: Keytype as NAI. NAI: name1@example.com
*Mar 20 12:10:11.975: [PMIPV6_BINDING_INFO]: binding found on NAI tree
*Mar 20 12:10:11.976: MIP_PDL_INFO: Route via: Ethernet0/0 (IPv6)
*Mar 20 12:10:11.976: MIP_PDL_INFO: Stopping LineProtoTimer for Tunnel1
*Mar 20 12:10:11.976: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel1, changed state
 to down
*Mar 20 12:10:11.976: MIP_PDL_INFO: Tunnel1 (IPv6) created with src 2001:DB8::1 dst 2006::4
*Mar 20 12:10:11.976: MIP_PDL_INFO: Successfully added route 172.16.0.0/12 to Tunnel1
*Mar 20 12:10:11.976: PMIPV6_LMA_INFO: Success in Adding IPv4 route (F0F0F06)
*Mar 20 12:10:11.976: MIP_PDL_INFO: Added Route to home addr. 2001:DB8::/64 via Tunnel
Tunnel1
*Mar 20 12:10:11.976: MIP_PDL_INFO: route_add success: 2
*Mar 20 12:10:11.976: PMIPV6_LMA_INFO: Added IPv6 route for HNP(2001:DB8::), Prefix Length(64)
*Mar 20 12:10:11.976: [PMIPV6_BINDING_INFO_KEY]: Keytype  as HOA. HOA: 0xF0F0F06
*Mar 20 12:10:11.976: [PMIPV6_BINDING_INFO]: pmipv6_update_binding_key, binding inserted
into HNP tree
*Mar 20 12:10:11.976: PMIPV6_LMA_INFO: Updated BCE(name1@example.com) with key(17) to Binding
 Module
*Mar 20 12:10:11.976: PMIPV6_LMA_INFO: Started Lifetime Timer(3600) sec for BCE
(name1@example.com)
*Mar 20 12:10:11.976: PMIPV6_LMA_INFO: Updated Lifetime (3600)secs for BCE(name1@example.com)
*Mar 20 12:10:11.976: PMIPV6_LMA_INFO: PBA Message to MAG:mag2 MN:name1@example.com ATT:4
SeqNo:362 Lifetime:3600 Status:0
*Mar 20 12:10:11.977: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel1, changed state
 to up
```

Related Commands

Command	Description
ipv6 mobile pmipv6-lma	Configures the LMA for the PMIP domain.

default profile

To enable the default profile for the mobile node (MN), use the **default profile** command in Local Mobility Anchor (LMA) configuration mode. To disable the default profile, use the **no** form of this command.

default profile *name*

no default profile *name*

Syntax Description

name	Profile name of the MN.

Command Default

The default profile is disabled.

Command Modes

LMA configuration (config-ipv6-pmipv6-lma)

Command History

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

Usage Guidelines

Use the **default profile** command, in LMA configuration mode, to enable the default profile for the MN.

When you configure the **default profile** command, if the locally configured profile or the profile that is fetched from the authentication, authorization, and accounting (AAA) server is unavailable in the MN, then the MN uses the default profile.

Examples

The following example shows how to configure the default profile for the MN:

```
Device(config-ipv6-pmipv6-domain)# nai example1@example.com
Device(config-ipv6-pmipv6-domain-mn)# network network1
Device(config-ipv6-pmipv6-domain-mn)# exit
Device(config-ipv6-pmipv6-domain)# exit
Device(config)# ipv6 mobile pmipv6-lma lma1 domain dn1
Device(config-ipv6-pmipv6-lma)# address ipv6 2001:DB8:0:0:E000::F
Device(config-ipv6-pmipv6-lma)# address ipv4 10.2.1.1
Device(config-ipv6-pmipv6-lma)# network network1
Device(config-ipv6-pmipv6lma-network)# pool ipv4 v4pool pfxlen 24
Device(config-ipv6-pmipv6lma-network)# pool ipv6 v6pool pfxlen 24
Device(config-ipv6-pmipv6lma-network)# exit
Device(config-ipv6-pmipv6-lma)# default profile example1@example.com
```

Related Commands

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

description (mobile networks)

To add a description to a mobile router configuration, use the **description**command in mobile networks configuration mode. To remove the description, use the **no** form of this command.

description *string*

no description

Syntax Description

string	Comment or description about the mobile router or its networks.

Command Default

No default behavior or values.

Command Modes

Mobile networks configuration

Command History

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

Usage Guidelines

The **description** command is meant solely as a comment to be put in the configuration to help you remember information about the configured mobile router or its mobile networks.

Examples

The following example shows how to add a description for the mobile router:

```
ip mobile mobile-networks 10.2.0.1
 description mobileunit
 network 172.6.1.0 255.255.255.0
 network 172.6.2.0 255.255.255.0
```

Related Commands

Command	Description
show ip mobile mobile-networks	Displays a list of mobile networks associated with the mobile router.

destination (IP multiplexing)

To specify the IPv4 or IPv6 destination address for the remote endpoint of an IP multiplexing path, use the **destination** command in IPv4 multiplexing profile configuration or IPv6 multiplexing profile configuration mode. To clear the destination address, use the **no** form of this command.

destination {*ip-addr*| *ipv6-addr*}

no destination

Syntax Description

ip-addr	IPv4 destination address for the remote endpoint of the IP multiplexing path.
ipv6-addr	IPv6 destination address for the remote endpoint of the IP multiplexing path.

Command Default

No destination address is configured.

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

You must configure a destination address for a profile in order to use it. If you attempt to issue a **no shutdown** command when no destination address is configured, you are prompted to configure a destination address. If a profile is active, you must issue a **shutdown** command before changing the destination address.

An incoming superframe must match its source and destination addresses to the destination and source addresses, respectively, in the multiplexing profile for the superframe to be demultiplexed. If either address does not match, the superframe is ignored.

After the destination address is specified, if you enter the **destination** command again, the new address overwrites the previously entered address.

Examples

The following example shows how to configure an IPv6 address as the destination address for superframe packets:

```
Router# configure terminal
```

```
Router(config)# ipv6 mux profile routeRTP-SJ
Router(config-ipmux-profile-v6)# destination FE80::A8BB:CCFF:FE01:5700
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.
shutdown	Deactivates an IP multiplexing profile.

discover-mn-detach

To enable the periodic verification of the mobile node (MN) attachment with the Mobile Access Gateway (MAG)-enabled interface, use the **discover-mn-detach** command in MAG configuration mode. To disable the periodic verification, use the **no** form of this command.

Cisco IOS XE Release 3.4S

discover-mn-detach *mn-attach-seconds timeout-seconds* **retries** *retry-count*

no discover-mn-detach

Cisco IOS XE Release 3.7S and Later Releases

discover-mn-detach poll interval*seconds* **timeout** *seconds* **retries** *retry-count*

no discover-mn-detach

Syntax Description

mn-attach-seconds	Period for verifying the MN attachment, in seconds. The range is from 1 to 100.
timeout-seconds	Timeout for response from the MN, in seconds. The timeout range is from 1 to 10, and should be less than the value for the period.
poll	Enables the Address Resolution Protocol (ARP).
interval *seconds*	Specifies the periodic time interval, in seconds, in which a MAG sends ARP requests to a MN. The range is from 11 to 36000. The default is 10.
timeout *seconds*	Specifies the timeout, in seconds, for a response from an MN. The range is from 1 to 10. The default is 2.
retries *retry-count*	Specifies a number of times a MAG retries sending ARP requests to an MN if the MAG does not receive any response from an MN. The range is from 1 to 10. The default is 0.

Command Default

The periodic verification of the MN attachment with the MAG-enabled interface is not enabled.

Command Modes

MAG configuration (config-ipv6-pmipv6-mag)

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.
Cisco IOS XE Release 3.7S	This command was modified. The **poll** keyword and the **retries** *retry-count* keyword-argument pair were added. The *seconds* argument was changed to **interval** *seconds* keyword-argument pair. The *timeout-seconds* argument was changed to **timeout** *seconds* keyword-argument pair.
15.2(4)M	This command was integrated into Cisco IOS Release 15.2(4)M.

Usage Guidelines

Use the **discover-mn-detach** command to enable the periodic verification of the MN attachment with the MAG-enabled interface. When periodic verification is enabled, the MAG periodically verifies the MN attachment by using the Address Resolution Protocol (ARP) request or the neighbor solicitation. When the mobile client responds with the ARP reply or the neighbor advertisement, a trigger attach is generated, thereby confirming that the MN is attached to the interface.

Examples

The following example shows how to periodically verify the MN attachment with the MAG-enabled interface:

```
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)# discover-mn-detach poll interval 11 timeout 3 retries 4
```

Related Commands

Command	Description
ipv6 mobile pmipv6-domain	Configures the PMIPv6 domain.
ipv6 mobile pmipv6-mag	Configures the MAG for the PMIPv6 domain.

dynamic mag learning

To enable local mobility anchor (LMA) to accept proxy mobile IPv6 (PMIPv6) signaling messages from any MAG that is not locally configured, use the **dynamic mag learning** command in LMA configuration mode. To enable the LMA to reject the PMIPv6 signaling messages from any MAG that is not locally configured, use the no form of the command.

dynamic mag learning

no dynamic mag learning

Syntax Description

This command does not have any arguments or keywords.

Command Default

LMA does not accept PMIPv6 signaling messages from any MAG that is not locally configured.

Command Modes

LMA configuration (config-ipv6-pmipv6-lma)

Command History

Release	Modification
Cisco IOS XE Release 3.8S	This command was introduced.

Examples

The following example shows how to enable the LMA to accept to PMIPv6 signaling messages

```
Device> enable
Device# configuration terminal
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)# dynamic mag learning
```

eigrp interface

Note Effective with Cisco IOS Release 15.0(1)M, the **eigrp interface**command is replaced by the **dampening-change** command and the **dampening-interval** command. See the **dampening-change** and **dampening-interval**commands for more information.

To set a threshold value to minimize hysteresis in a router-to-radio configuration, use the **eigrp interface** command in interface configuration mode. To reset the hysteresis threshold to the default value, use the **no** form of this command.

eigrp *vmi-interface-number* **interface** [**dampening-change** *value*] [**dampening-interval** *value*]

no eigrp *vmi-interface-number* **interface** [**dampening-change** *value*] [**dampening-interval** *value*]

Syntax Description

vmi-interface-number	The number assigned to the VMI interface.
dampening-change *value*	(Optional) Value used to minimize the effect of frequent routing changes in router-to-radio configurations. Percent interface metric must change to cause update. Value range is 1 to 100.
dampening-interval *value*	(Optional) Specifies the time interval in seconds to check the interface metrics at which advertising of routing changes occurs. The default value is 30 seconds. Value range is 1 to 65535.

Command Default

Default for change-based dampening is 50 percent of the computed metric.

Default for interval-based dampening is 30 seconds.

Command Modes

Interface configuration (config-if)

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.
15.0(1)M	This command was replaced. This command was replaced by the **dampening-change**command and the **dampening-interval** command.

Usage Guidelines

This command advertises routing changes for EIGRP traffic only.

The REPLY sent to any QUERY will always contain the latest metric information. Exceptions which will result in immediate UPDATE being sent:

- A down interface
- A down route
- Any change in metric which results in the router selecting a new next hop

Change-based Dampening

The default value for the change tolerance will be 50% of the computed metric. It can be configured in the range from 0 to 100 percent. If the metric change of the interface is not greater (or less) than the current metric plus or minus the specified amount, the change will not result in a routing change, and no update will be sent to other adjacencies.

Interval-based Dampening

The default value for the update intervals is 30 seconds. It can be configured in the range from 0 to 64535 seconds. If this option is specified, changes in routes learned though this interface, or in the interface metrics, will not be advertised to adjacencies until the specified interval is met. When the timer expires, any changes detected in any routes learned through the interface, or the metric reported by the interfaces will be sent out.

Examples

Examples

The following example sets the threshold to 50 percent tolerance routing updates involving VMI interfaces and peers:

```
interface vmi1
 ip address 10.2.2.1 255.255.255.0
 ipv6 address 2001:0DB1:2::1/96
 ipv6 enable
 eigrp 1 interface dampening-change 50
 physical-interface Ethernet0/0
```

Examples

The following example sets the interval to 30 seconds at which updates occur for topology changes that affect VMI interfaces and peers:

```
interface vmi1
 ip address 10.2.2.1 255.255.255.0
 ipv6 address 2001:0DB1:2::1/96
 ipv6 enable
 eigrp 1 interface dampening-interval 30
 physical-interface Ethernet0/0
```

Related Commands

Command	Description
debug vmi	Displays debugging output for virtual multipoint interfaces (VMIs)

Command	Description
interface vmi	Creates a virtual multipoint interface (VMI) that can be configured and applied dynamically.

enable aaa accounting

To enable authentication, authorization, and accounting (AAA) accounting for mobile node (MN) sessions, use the **enable aaa accounting** command in LMA configuration mode. To disable AAA accounting, use the **no** form of this command.

enable aaa accounting

no enable aaa accounting

Syntax Description

This command has no arguments or keywords.

Command Default

AAA accounting is disabled.

Command Modes

LMA configuration mode (config-ipv6-pmipv6-lma)

Command History

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

Usage Guidelines

Use the **enable aaa accounting** command to enable AAA accounting for MN sessions. Only when AAA accounting is enabled, the LMA sends start or stop accounting notification to the AAA server when a binding for the MN is created or deleted in the LMA.

Examples

The following example shows how to enable AAA accounting in an LMA:

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

Related Commands

Command	Description
ipv6 mobile pmipv6-lma	Configures the LMA for the PMIP domain.

enable sessionmgr

To enable mobile client service abstraction (MCSA) to receive notifications from Intelligent Services Gateway (ISG), use the **enable sessionmgr** command in MCSA configuration mode. To disable this functionality, use the **no** form of this command.

enable sessionmgr

no enable sessionmgr

Syntax Description

This command has no arguments or keywords.

Command Default

MCSA does not receive notifications from ISG.

Command Modes

MCSA configuration (config-mcsa)

Command History

Release	Modification
Cisco IOS XE Release 3.8S	This command was introduced.

Usage Guidelines

Use the **show mcsa statistics sint** command to verify if the MCSA has received any notification from the ISG.

Examples

The following example shows how to enable the MCSA to receive notifications from ISG:

```
Device> enable
Device# configuration terminal
Device(config-if) mcsa
Device(config-mcsa) enable sessionmgr
Device(config-mcsa) end
```

Related Commands

Command	Description
show mcsa statistics sint	Displays the MCSA notifications statistics.

encap (proxy mobile IPv6)

To configure the tunnel encapsulation type for a PMIP domain, for a Local Mobility Anchor (LMA) with a Mobile Access Gateway (MAG), or for a MAG within an LMA, use the **encap** command in the appropriate configuration mode. To disable the tunnel encapsulation mode type, use the **no** form of this command.

encap {**gre-ipv4** | **gre-ipv6** | **ipv6-in-ipv6** | **udptunnel**}

no encap {**gre-ipv4** | **gre-ipv6** | **ipv6-in-ipv6** | **udptunnel**}

Syntax Description

gre-ipv4	Sets the tunnel encapsulation type to generic routing encapsulation (GRE) in IPv4.
gre-ipv6	Sets the tunnel encapsulation type to GRE in IPv6.
ipv6-in-ipv6	Sets the tunnel encapsulation type to IPv6 in IPv6.
udptunnel	Sets the tunnel encapsulation type to UDP.

Command Default

The Proxy Mobile IPv6 (PMIPv6) tunnel encapsulation mode type is IPv6 in IPv6.

Command Modes

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

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

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

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 MAG-LMA configuration mode.
15.2(4)M	This command was integrated into Cisco IOS Release 15.2(4)M.
Cisco IOS XE Release 3.6S	This command was modified. This **udptunnel** keyword was added.

Usage Guidelines

Use the **encap** command in PMIPV6 domain configuration mode to configure the tunnel encapsulation type for the PMIPV6 domain. The LMAs and the MAGs within the PMIPV6 domain use this configuration as the default.

Note You can configure the UDP encapsulation type only in PMIPv6 domain configuration mode, whereas you can configure other encapsulation types in PMIPv6 domain configuration, MAG-LMA configuration and LMA-MAG configuration modes.

Use the **encap** command in MAG-LMA configuration mode to configure the tunnel encapsulation type for the LMA within the MAG.

Use the **encap** command in LMA-MAG configuration mode to configure the tunnel encapsulation type for the MAG within the LMA.

Examples

The following example shows how to configure the encapsulation type as IPv6 in IPv6 in MAG-LMA configuration mode:

```
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)# encap ipv6-in-ipv6
```

The following example shows how to configure an encapsulation type in LMA-MAG configuration mode:

```
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)# encap ipv6-in-ipv6
```

The following example shows how to configure an encapsulation type in PMIPV6 domain configuration mode:

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

Related Commands

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

fixed-link-layer-address

To configure the fixed link-layer address (Layer 2 address) for the Mobile Access Gateway (MAG)-enabled interface toward the mobile node (MN), use the **fixed-link-layer-address** command in PMIPV6 domain or MAG configuration mode. To remove the fixed Layer 2 address for the MAG-enabled interface, use the **no** form of this command.

fixed-link-layer-address *hardware-address*

no fixed-link-layer-address

Syntax Description

hardware-address	The 48-bit hardware address.

Command Default

No fixed link-layer address is configured.

Command Modes

MAG configuration (config-ipv6-pmipv6-mag)

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 **fixed-link-layer-address** command in PMIPV6 domain configuration mode to configure the fixed link layer address for the MAG-enabled interface within the PMIPv6 domain. If the PMIPv6 domain is configured using the **ipv6 mobile pmipv6-domain** *domain-name* **load-aaa** command, use the **fixed-link-layer-address** command to override the fixed link layer address configuration.

Use the **fixed-link-layer-address** command in MAG configuration mode to configure the fixed link-layer address for the MAG-enabled interface.

Examples

The following example shows how to configure the fixed link layer address for the MAG-enabled interface toward the MN in PMIPV6 domain configuration mode:

```
Device(config)# ipv6 mobile pmipv6-domain dn1
Device(config-ipv6-pmipv6-domain)# fixed-link-layer-address aaaa.bbbb.cccc
```

The following example shows how to configure the fixed link layer address for the MAG-enabled interface in MAG configuration mode:

```
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)# fixed-link-layer-address aaaa.bbbb.cccc
```

Related Commands

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

fixed-link-local-address

To configure the fixed link-local address for the Mobile Access Gateway (MAG)-enabled interface toward the mobile node (MN), use the **fixed-link-local-address** command in PMIP domain or MAG configuration mode. To remove the fixed link-local address on the MAG-enabled interface, use the **no** form of this command.

fixed-link-local-address *ipv6-address*

no fixed-link-local-address

Syntax Description

ipv6-address	The IPv6 link-local address assigned to the MAG-enabled interface toward the MN.

Command Default

No fixed link-local address is configured for the MAG-enabled interface toward the MN.

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.

Usage Guidelines

Use the **fixed-link-local-address** command in the PMIP domain configuration mode to configure the fixed link-local address for the MAG-enabled interface within the Proxy Mobile IPv6 (PMIP) domain. If the PMIP domain is configured using **ipv6 mobile pmipv6-domain** *domain-name* **load-aaa** command, use the **fixed-link-local-address** command to override the fixed link-local address configuration.

Use the **fixed-link-local-address** command in MAG configuration mode to configure the fixed link-local address for the MAG-enabled interface.

Examples

The following example shows how to configure the fixed link-local address for the MAG-enabled interface toward the MN in PMIP domain configuration mode:

```
Router(config)# ipv6 mobile pmipv6-domain dn1
Router(config-ipv6-pmipv6-domain)# fixed-link-local-address FE80:0DB8:3333:4::5
```

The following example shows how to configure the fixed link-local address for the MAG-enabled interface 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)# fixed-link-local-address FE80:0DB8:3333:4::5
```

Related Commands

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

generate grekey

To dynamically generate upstream or downstream generic routing encapsulation (GRE) keys for mobile nodes (MNs) in a local mobile anchor (LMA) or a mobile access gateway (MAG) respectively, use the **generate grekey** command in MAG or LMA configuration mode respectively. To disable the dynamic generation of upstream or downstream GRE keys in an LMA or MAG, use the **no** form of this command.

generate grekey

no generate grekey

Syntax Description

This command has no arguments or keywords.

Command Default

The upstream or the downstream GRE keys for the MNs in the LMA or MAG respectively are generated dynamically.

Command Modes

MAG configuration (config-ipv6-pmipv6-mag)

LMA configuration (config-ipv6-pmipv6-lma)

Command History

Release	Modification
Cisco IOS XE Release 3.8S	This command was introduced.

Usage Guidelines

When you enter the **no generate key** command in the LMA or MAG configuration mode, the upstream or downstream GRE keys for the MNs are not generated dynamically. In that case, you must use the keys from the authentication, authorization, and accounting (AAA) profile or the local mobile node (MN) configuration.

When tunnel encapsulation mode in the configured MAG is GRE-IPv4, it is required that every mobile subscriber should have a GRE key. To provide every mobile subscriber with a GRE key value, perform one of the following:

- Enter the **generate grekey** in MAG configuration mode. The GRE key value, thus generated, are assigned to every mobile subscriber as and when the mobile subscribers attach to the MAG.
- Explicitly assign the GRE key values to the Network Access Identifier (NAI) in the PMIPv6 domain.
- Configure the GRE key for each subscriber in the AAA attributes.

Examples

The following example shows how to dynamically generate upstream GRE keys for MNs in an LMA:

```
Device> enable
Device(config)# ipv6 mobile pmipv6-mag mag1 domain dn1
Device(config-ipv6-pmipv6-mag)# no generate grekey
Device(config-ipv6-pmipv6-mag)# end
```

The following example shows how to explicitly configure GRE key to NAI to generate downstream GRE keys.

```
Device> enable
Device# configuration terminal
Device(config)# ipv6 mobile pmipv6-domain dn1
Device(config-ipv6-pmipv6-domain)# nai user1@example.com
Device(config-ipv6-pmipv6-domain-mn)# gre-encap-key up 100
Device(config-ipv6-pmipv6-domain-mn)# gre-encap-key down 200
Device(config-ipv6-pmipv6-domain-mn)# end
```

Related Commands

Command	Description
gre-encap-key	Configures the GRE key for the MN.
nai	Configures the NAI for the MN within the PMIPV6 domain.

gre-encap-key

To configure the generic routing encapsulation (GRE) key for the mobile node (MN), use the **gre-encap-key** command in Proxy Mobile IPv6 (PMIPV6) domain mobile node configuration mode. To remove the configuration, use the **no** form of this command.

gre-encap-key [**down** *key-value*| **up** *key-value*]

no gre-encap-key [**down**| **up**]

Syntax Description

down *key-value*	(Optional) Specifies the encapsulation key as downstream from the Local Mobility Anchor (LMA) to the Mobile Access Gateway (MAG). The range for the *key-value* argument is from 0 to 4294967295.
up *key-value*	(Optional) Specifies the encapsulation key as upstream from the MAG to the LMA. The range for the *key-value* argument is from 0 to 4294967295.

Command Default

No GRE key is configured.

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 configure a GRE key from the LMA to the MAG:

```
Device(config)# ipv6 mobile pmipv6-domain dn1
Device(config-ipv6-pmipv6-domain)# nai example@example.com
Device(config-ipv6-pmipv6-domain-mn)# gre-encap-key down 45
```

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.

heartbeat

To configure heartbeat detection between Mobile Access Gateway (MAG) and Local Mobility Anchor (LMA), use the heartbeat command in LMA configuration mode. To disable heartbeat detection, use the **no** form of this command.

heartbeat [**interval** *interval*] **retries** *retries* [**label** *label*] [**natreboot**]

no heartbeat [**interval** *interval*] **retries** *retries* [**label** *label*] [**natreboot**]

Syntax Description

interval *interval*	Specifies the interval for the heartbeat, in seconds. The range is from 1 to 3600.
retries *retries*	Specifies the number of heartbeat retries. The range is from 1 to 10.
label *label*	Specifies the path label of the MAG's roaming interface.
natreboot	Specifies the NAT reboot detection.

Command Default

There is no heartbeat detection between MAG and LMA.

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 specify the heartbeat interval, retries, labels and NAT reboot detection:

```
Device(config)# ipv6 mobile pmipv6-lma lma1 domain dn1
Device(config-ipv6-pmipv6-lma)# heartbeat interval 300 retries 2 label label1 natreboot
```

home interface

To enable a specific interface as the home interface for a logical mobile node (LMN), use the **home interface** command in MAG logical-mn configuration mode. To disassociate a home interface from a logical mobile node, use the **no** form of this command.

home interface*type number*

Syntax Description

type	Interface type that is configured as the home interface. **Note** The home interface should be of the interface type loopback only.
number	Interface number.

Command Default

The home interface is not configured.

Command Modes

MAG logical MN configuration (config-ipv6-pmipv6-mag-logicalmn)

Command History

Release	Modification
15.4(1)T	This command was introduced.

Usage Guidelines

Network Access Identifier (NAI) should already be configured under the PMIPv6 domain configuration mode.

Examples

The following example shows how to enable the mobile router:

```
Device(config)# ipv6 mobile pmipv6-mag mag1 domain dn1
Device(config-ipv6-pmipv6-mag)# logical-mn mn1@example.com
Device(config-ipv6-pmipv6-mag-logicalmn)# home interface loopback 0
```

holdtime

To specify the amount of time, in milliseconds, that a multiplexing profile waits to fill a superframe before sending a partial superframe with currently queued packets, use the **holdtime** 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.

holdtime *milliseconds*

no holdtime

Syntax Description

milliseconds	Amount of time, in milliseconds, that a multiplexing profile waits before sending a partial superframe. The range is 20 to 250.

Command Default

The default holdtime is 20 milliseconds.

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 enter a holdtime, the profile waits the default value of 20 milliseconds before sending a partial superframe.

Examples

The following example shows how to configure the holdtime to 150 milliseconds before the profile forwards a partial superframe:

```
Router# configure terminal
Router(config)# ipv6 mux profile routeRTP-SJ
Router(config-ipmux-profile-v6)# holdtime 150
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.

home-agent

To specify the home agent that the mobile router uses during registration, use the **home-agent** command in mobile router configuration mode. To disable the home agent, use the **no** form of this command.

home-agent *ip-address* [**priority** *level*]

no home-agent *ip-address* [**priority** *level*]

Syntax Description

ip-address	Home IP address.
priority *level*	(Optional) Priority level that prioritizes which home agent address is the best to use during registration. The range is from 0 to 255, where 0 denotes the lowest priority and 255 denotes the highest priority. The default is 100.

Command Default

The default priority level is 100.

Command Modes

Mobile router configuration

Command History

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

Usage Guidelines

The **home-agent** command specifies which home agent the mobile router uses for registration and to de tect when it is home. The priority level determines which home agent address to register with, although all addresses are on the same home agent. The mobile router registers with the home agent with the highest priority level.

The home agent address list is used to detect when the mobile router is home. The mobile router knows that it is at home when the source of the agent advertisements is an IP source address that exists on the home agent address list.

Examples

The following example shows that the mobile router will use the home agent address 1.1.1.1 during registration and will detect when it is at home after receiving agent advertisements from either address 1.1.1.1 or 2.2.2.2:

```
router mobile
ip mobile router
  address 10.1.0.1 255.255.0.0
  home-agent 1.1.1.1 priority 101
  home-agent 2.2.2.2 priority 100
```

Related Commands

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

int att

To configure the access technology type (ATT), the interface, and the MAC address of the mobile node (MN) interface, use the **int att** command in PMIPV6 domain mobile node configuration mode. To remove the configuration of the MN, use the **no** form of this command.

int att *interface-access-type* **l2-addr** *mac-address*

no int att *interface-access-type* **l2-addr** *mac-address*

Syntax Description

interface-access-type	MN interface access technology type. The type can be **ethernet** , **PPP**, **virtual**, **wima**, or **wlan**.
l2-addr	Specifies the MAC address of the MN interface.
mac-address	MAC address of the MN interface.

Command Default

The ATT, interface type, and MAC address are not configured 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 configure the ATT, interface type, and MAC address of the MN interface:

```
Device(config)# ipv6 mobile pmipv6-domain dn1
Device(config-ipv6-pmipv6-domain)# nai example@example.com
Device(config-ipv6-pmipv6-domain-mn)# int att ETHERNET l2-addr 02c7.f800.0422
```

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.

interface (proxy mobile IPv6)

To configure the interface on which Mobile Access Gateway (MAG) functionality or third-generation mobility anchor (3GMA) functionality is enabled, or to configure the interface on which the mobile maps is to be applied on Local Mobility Anchor (LMA), use the **interface** command in appropriate configuration mode. To remove the interface configuration, use the **no** form of this command.

interface *type number*

no interface *type number*

Syntax Description

type	Type of interface to be configured.
number	Port, connector, or interface card number.

Command Default

MAG or 3GMA functionality for the interface is not configured, or the mobile maps are not applied on LMA.

Command Modes

LMA configuration (config-ipv6-pmipv6-lma)

MAG configuration (config-ipv6-pmipv6-mag)

3GMA role configuration (config-ipv6-pmipv6lma-role)

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.
Cisco IOS XE Release 3.9S	This command was modified. This command was made available in 3GMA configuration mode.
Cisco IOS XE Release 3.10S	This command was modified. This command was made available in LMA configuration mode and is enhanced to apply mobile maps.

Usage Guidelines

When mobile nodes are used in dual stack mode with IPv4 transport between MAG and LMA, either enable IPv6 on the access interface of MAG using the **ipv6 enable** command in interface configuration mode, or explicitly configure an IPv6 address on the MAG access interface.

Examples

The following example shows how to enable Gigabit Ethernet 0/1/0 interface for 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)# interface GigabitEthernet 0/1/0
```

The following example shows how to enable Gigabit Ethernet 0/1/0 interface for the 3GMA:

```
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)# interface GigabitEthernet 0/1/0
```

The following example shows how to enable Gigabit Ethernet 0/1/0 interface for the mobile maps:

```
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)# role 3gma
Device(config-ipv6-pmipv6lma-role)# interface GigabitEthernet 0/1/0
```

Related Commands

Command	Description
ipv6 enable	Enables IPv6 processing on an interface that has not been configured with an explicit IPv6 address.
ipv6 mobile pmipv6-domain	Configures the PMIPV6 domain.
ipv6 mobile pmipv6-mag	Configures the MAG for the PMIPV6 domain.
ipv6 mobile pmipv6-lma	Configures the LMA for the PMIPV6 domain.

ip dampening-change eigrp

To set a threshold percentage to minimize or dampen the effect of frequent routing changes through an interface in Enhanced Interior Gateway Routing Protocol (EIGRP) for IPv4, use the **ip dampening-change eigrp**command in interface configuration mode. To restore the default value, use the **no** form of this command.

ip dampening-change eigrp *as-number* [*change-percentage*]

no ip dampening-change eigrp *as-number*

Syntax Description

as-number	Autonomous system number. The range is from 1 to 65535.
change-percentage	(Optional) The percentage a metric must change before the value is stored for future decisions on advertisements. The range is from 1 to 100. If a change-percentage value is not specified, the default is 50 percent of the computed metric.

Command Default

No threshold percentage is configured.

Command Modes

Interface configuration (config-if) Virtual network interface (config-if-vnet)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.
Cisco IOS XE Release 3.2S	This command was modified. Support was added for this command in virtual network interface configuration mode.

Usage Guidelines

The **ip dampening-change eigrp** command is supported only for Mobile Ad Hoc Networking (MANET) router-to-radio links.

When a peer metric changes on an interface that is configured with the **ip dampening-change eigrp**command, EIGRP multiplies the dampening-change percentage with the old peer metric and compares the result (the threshold) to the difference between the old and new metrics. If the metric difference is greater than the calculated threshold, then the new metric is applied and the routes learned from that peer are updated and advertised to other peers. If the metric difference is less than the threshold, the new metric is discarded.

The following are the exceptions that will result in an immediate update of the routes regardless of the dampening-change setting:

- An interface is down.
- A route is down.
- A change in the metric that results in the router selecting a new next hop.

Peer metric changes that do not exceed a configured change percentage and that do not result in a routing change do not cause an update to be sent to other adjacencies. Peer metric changes are based on the stored last-update of the peer. Peer metric changes that exceed the threshold value are stored and used for future comparisons.

Examples

The following example shows how to configure the EIGRP to accept a peer metric change if the change is greater than 75 percent of the last updated value:

```
Router(config)# interface fastethernet 0/0
Router(config-if)# ip dampening-change eigrp 1 75
```

Related Commands

Command	Description
dampening-interval	Sets a threshold time interval to minimize or dampen the effect of frequent routing changes through an interface in an EIGRP address family or service family.
dampening-change	Sets a threshold percentage to minimize or dampen the effect of frequent routing changes through an interface in an EIGRP address family or service family.
ip dampening-interval	Sets a threshold time interval to minimize or dampen the effect of frequent routing changes through an interface in EIGRP for IPv4.
ipv6 dampening-change	Sets a threshold percentage to minimize or dampen the effect of frequent routing changes through an interface in EIGRP for IPv6.
ipv6 dampening-interval	Sets a threshold time interval to minimize or dampen the effect of frequent routing changes through an interface in EIGRP for IPv6.

ip dampening-interval eigrp

To set a threshold time interval to minimize or dampen the effect of frequent routing changes through an interface in Enhanced Interior Gateway Routing Protocol (EIGRP) for IPv4, use the **ip dampening-interval eigrp** command in interface configuration mode. To restore the default value, use the **no** form of this command.

ip dampening-interval eigrp *as-number* [*interval*]

no ip dampening-interval eigrp *as-number*

Syntax Description

as-number	Autonomous system number. The range is from 1 to 65535.
interval	(Optional) Time interval, in seconds, that must elapse before a route change will cause an update to occur. The range is from 1 to 65535. If an *interval*value is not specified, the default is 30 seconds.

Command Default

A dampening interval is not enabled.

Command Modes

Interface configuration (config-if) Virtual network interface (config-if-vnet)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.
Cisco IOS XE Release 3.2S	This command was modified. Support was added for this command in virtual network interface configuration mode.

Usage Guidelines

The **ip dampening-interval eigrp**command is supported only for Mobile Ad Hoc Networking (MANET) Router-to-Radio links.

When a peer metric changes on an interface that is configured with a dampening interval, EIGRP for IPv4 will apply the metric change only if the time difference since the last metric change exceeds the specified interval. If the time difference is less than the specified interval, the update is discarded.

The following are the exceptions that result in an immediate update of the routes regardless of the dampening interval settings:

- An interface is down.
- A route is down.

- A change in the metric that results in the router selecting a new next hop.

Examples

The following example shows how to configure EIGRP for IPv4 on a FastEthernet interface 0/0 to limit the metric change frequency to no more than one change in a 45-second interval:

```
Router(config)# interface fastethernet 0/0
Router(config-if)# ip dampening-interval eigrp 1 45
```

Related Commands

Command	Description
dampening-change	Sets a threshold percentage to minimize or dampen the effect of frequent routing changes through an interface in an EIGRP address family or service family.
dampening-interval	Sets a threshold time interval to minimize or dampen the effect of frequent routing changes through an interface in an EIGRP address family or service family.
ip dampening-change	Sets a threshold percentage to minimize or dampen the effect of frequent routing changes through an interface in EIGRP for IPv4.
ipv6 dampening-change	Sets a threshold percentage to minimize or dampen the effect of frequent routing changes through an interface in EIGRP for IPv6.
ipv6 dampening-interval	Sets a threshold time interval to minimize or dampen the effect of frequent routing changes through an interface in EIGRP for IPv6.

ip dhcp client mobile renew

To configure the number of renewal attempts and the interval between attempts for renewing an IP address acquired by a Dynamic Host Configuration Protocol (DHCP) client, use the **ip dhcp client mobile renew** command in interface configuration mode. To disable the functionality, use the **no** form of this command.

ip dhcp client mobile renew count *number* **interval** *ms*

no ip dhcp client mobile renew count *number* **interval** *ms*

Syntax Description

count *number*	Number of attempts to renew a current IP address before starting the DHCP discovery process. The range is from 0 to 10 attempts. The default is 2 attempts.
interval *ms*	Interval to wait between renewal attempts. The range is from 1 to 1000 ms. The default is 50 ms.

Command Default

count *number* : 2**interval** *ms*: 50

Command Modes

Interface configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

Mobile DHCP clients automatically attempt to renew an existing IP address in response to certain events, such as moving between wireless access points. The number of renewal attempts, and the interval between those attempts, depending on network conditions, can be modified by using the **ip dhcp client mobile renew** command.

Examples

In the following example, the DHCP client will make four attempts to renew its current IP address with an interval of 30 milliseconds between attempts :

```
interface FastEthernet0
 ip dhcp client mobile renew count 4 interval 30
```

Related Commands

Command	Description
ip address dhcp	Acquires an IP address on an interface from DHCP.

ip mobile arp

To enable local-area mobility, use the **ip mobile arp** command in interface configuration mode. To disable local-area mobility, use the **no** form of this command.

ip mobile arp [**timers** *keepalive hold-time*] [**access-group** *access-list-number*| *name*]

no ip mobile arp

Syntax Description

timers	(Optional) Sets local-area mobility timers.
keepalive	(Optional) Frequency, in minutes, at which the Cisco IOS software sends unicast Address Resolution Protocol (ARP) messages to a relocated host to verify that the host is present and has not moved. The default value is 5.
hold-time	(Optional) Hold time, in minutes. This is the length of time the software considers that a relocated host is present without receiving some type of ARP broadcast or unicast from the host. Normally, the hold time should be at least three times greater than the keepalive time. The default value is 15.
access-group	(Optional) Indicates that you are applying an access list. This access list applies only to local-area mobility.
access-list-number	(Optional) Number of a standard IP access list. The range is from 1 to 99. Only hosts with addresses permitted by this access list are accepted for local-area mobility.
name	(Optional) Name of an IP access list. The name cannot contain a space or quotation mark, and must begin with an alphabetic character to avoid ambiguity with numbered access lists.

Command Default

Local-area mobility is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
XE 2.5.1	This command was integrated into Cisco IOS XE Release 2.5.1. VRF-awareness for local-area mobility is available in this release.

Usage Guidelines

Local-area mobility is supported on Ethernet, Token Ring, and FDDI interfaces only.

To create larger mobility areas, you must first redistribute the mobile routes into your Interior Gateway Protocol (IGP). The IGP must support host routes. You can use Enhanced IGRP, Open Shortest Path First (OSPF), or Intermediate System-to-Intermediate System (IS-IS); you can also use Routing Information Protocol (RIP), but RIP is not recommended. The mobile area must consist of a contiguous set of subnets.

Using an access list to control the list of possible mobile nodes is strongly encouraged. Without an access list, misconfigured hosts can be mistaken for mobile nodes and disrupt normal operations.

Examples

The following example shows how to configure local-area mobility on Ethernet interface 0:

```
access-list 10 permit 10.92.37.114
 interface ethernet 0
 ip mobile arp access-group 10
```

Related Commands

Command	Description
access-list (IP standard)	Defines a standard IP access list.
default-metric (BGP)	Sets default metric values for the BGP, OSPF, and RIP routing protocols.
default-metric (OSPF)	Sets default metric values for OSPF.
default-metric (RIP)	Sets default metric values for RIP.
network (BGP)	Specifies the list of networks for the BGP routing process.
network (IGRP)	Specifies a list of networks for the IGRP or Enhanced IGRP routing process.

Command	Description
network (RIP)	Specifies a list of networks for the RIP routing process.
redistribute (IP)	Redistributes routes from one routing domain into another routing domain.
router eigrp	Configures the IP Enhanced IGRP routing process.
router isis	Enables the IS-IS routing protocol and specifies an IS-IS process for IP.
router ospf	Configures an OSPF routing process.

ip mobile authentication ignore-spi

To enable the home agent or foreign agent to accept RFC-2002 based mobile nodes or foreign agents that don’t include the security parameter index (SPI) in the authentication extension of the registration message, use the ip mobile authentication ignore-spi command in global configuration mode. To disable this functionality, use the **no** form of this command.

ip mobile authentication ignore-spi

no ip mobile authentication ignore-spi

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

Global configuration.

Command History

Release	Modification
12.2(8)BY	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

Usage Guidelines

Cisco IOS software supports the Mobile-Home Authentication Extension (MHAE). All registration messages between a mobile and a home agent include a mandatory authentication extension.

In RFC 2002, the SPI field was not included to calculate the authenticator value in the authentication extension of the registration message. In RFC 3220 and 3344, the SPI field in the authentication extension is used as part of the data over which the authentication algorithm must be computed.

The command turns off authentication and allows an RFC-2002 based mobile node and foreign agent to register with the home agent even though the SPI field is not included in the authentication extension of the registration message. The foreign agent will accept both RFC 2002 and RFC 3220/3344 based visitors and the home agent will accept both RFC 2002 and RFC 3220/3344 based mobile nodes and foreign agents.

Examples

The following example allows the home agent to accept registration messages without the SPI in the authentication extension:

```
ip mobile authentication ignore-spi
```

ip mobile bindupdate

To enable a home agent to send a binding update message to a foreign agent, use the **ip mobile bindupdate** command in global configuration mode. To disable this functionality, use the **no** form of this command.

ip mobile bindupdate [acknowledge] [**maximum** *seconds*] [**minimum** *seconds*] [**retry** *number*]

no ip mobile bindupdate [acknowledge] [**maximum** *seconds*] [**minimum** *seconds*] [**retry** *number*]

Syntax Description

acknowledge	(Optional). Indicates that the foreign agent must acknowledge receipt of a binding update message.
maximum *seconds*	(Optional) Maximum period (in seconds) that the home agent waits before retransmission of a binding update message. The default is 10 seconds.
minimum *seconds*	(Optional) Minimum period (in seconds) that the home agent waits before retransmission of a binding update message. The default is 1 second.
retry *number*	(Optional) Number of times to retry sending the binding update message. Retransmission stops after the maximum number of retries are attempted. The range is from 1 to 4; the default retry is 4.

Command Default

maximum *seconds* : 10 seconds**minimum** *seconds*: 1 second**retry** *number*: 4 retries

Command Modes

Global configuration

Command History

Release	Modification
12.2(8)BY	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

Usage Guidelines

This command enables the home agent to send a binding update message to the previous foreign agent when the mobile node moves to a new care-of address. The binding update message informs the foreign agent that a mobile node has moved and it can reclaim resources associated with that mobile node such as a visitor entry or visitor route.

Typically, resources on the foreign agent are not reclaimed until the mobility binding lifetime expires for that mobile node. By using this command, the foreign agent does not have to wait to reclaim resources used by the mobile node when that mobile node is no longer associated with the foreign agent.

Without this command configured, when a mobile node moves from foreign agent 1 to foreign agent 2 or when the home agent removes the binding, foreign agent 1 does not know that the mobile node has moved and the resources on foreign agent 1 associated with the mobile node will not be cleared until the lifetime expires for the mobile node.

If the **acknowledge** keyword is specified, the home agent periodically retransmits a binding update message until it receives a binding acknowledgement from the foreign agent or until the number of retries is exceeded.

The home agent and foreign agent must share a security association. The binding update message from the home agent and the binding update acknowledgement from the foreign agent must contain a FHAE (Foreign-Home Authentication Extension). If the FHAE is not configured on the home agent with the **ip mobile secure** command, the home agent will not send a binding update message even if the **ip mobile bindupdate** command is configured.

Examples

The following example configures the home agent to wait a maximum of 8 seconds before retransmitting a binding update message to a foreign agent. The foreign agent must send an acknowledgement of this binding update message upon receipt.

```
ip mobile bindupdate acknowledge maximum 8 retry 3
ip mobile secure foreign-agent 10.31.1.1 spi 100 key hex 23456781234567812345678123456781
```

The following example configures the security association on the foreign agent. Without the security association configured on the home agent and the foreign agent, the binding update message would not be sent or processed.

```
ip mobile secure home-agent 172.31.10.1 spi 100 key hex 23456781234567812345678123456781
```

ip mobile cdma ha-chap send attribute

To include the Mobile Equipment Identifier (MEID) in the HA-CHAP access request, use the ip mobile cdma ha-chap send attribute command in global configuration mode. To disable this feature, use the no form of the command.

ip mobile cdma ha-chap send attribute [**A1**| **A2**| **A3**]

no ip mobile cdma ha-chap send attribute [**A1**| **A2**| **A3**]

Syntax Description

A1	(Optional) Send A1 (Calling Station ID) in ha-chap.
A2	(Optional) Send A2 (ESN) in ha-chap.
A3	(Optional) Send A3 (MEID) in ha-chap.

Command Default

There are no default values.

Command Modes

Global configuration

Command History

Release	Modification
12.3(14)YX1	This command was introduced.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.

Usage Guidelines

The MEID is a new attribute introduced in IS-835D that will eventually replace the ESN. In the interim, both attributes are supported on the Home Agent.

The MEID NVSE will be appended by the PDSN node to the Mobile IP RRQ. When the MEID NVSE is received on the HA, and the ip mobile cdma ha-chap send attribute A3 command is configured, then the MEID value is included in the HA-CHAP access request.

Examples

The following example illustrates the ip mobile cdma ha-chap send attribute A3 command:

```
ip mobile cdma ha-chap send attribute A3
```

ip mobile debug include username

To display the user name or International Mobile Subscriber Identity (IMSI) condition with each debug statement, use the ip mobile debug include username command. To remove the user name or IMSI condition from the debug display, use the no form of the command.

ip mobile debug include username

no ip mobile debug include username

Syntax Description

This command has no arguments or keywords.

Command Default

The user name or IMSI condition is not displayed in the debug output.

Command Modes

Global configuration

Command History

Release	Modification
12.3(14)YX	This command was introduced.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.

Usage Guidelines

In the following example, the user name or IMSI condition will be displayed in any Mobile IP debug output:

```
Router(config)# ip mobile debug include username
```

ip mobile foreign-agent

To enable foreign agent service, use the **ip mobile foreign-agent**command inglobal configuration mode. To disable this service, use the **no** form of this command.

ip mobile foreignagent [**careof interface [interface-only] [transmit-only]| reg-wait** *seconds***| local-timezone| reverse-tunnel private-address**]

no ip mobile foreignagent [**careof interface [interface-only] [transmit-only]| reg-wait| local-timezone| reverse-tunnel private-address**]

Syntax Description

care-of *interface*	IP address of the interface. Sets the care-of address on the foreign agent. Multiple care-of addresses can be configured. At least one care-of address must be configured for foreign agent service.
interface-only	(Optional) Enables the specified interface to advertise only its own address as the care-of address. Other interfaces configured for foreign agent service will not advertise this care-of address.
transmit-only	(Optional) Informs Mobile IP that the *interface* is being used on a unidirectional link and will transmit only. This interface will be used as the source interface for this care-of address for any registration request received on another interface. Only serial interfaces can be configured as transmit only.
reg-wait *seconds*	(Optional) Pending registration expires after *the specified number of* seconds if no reply is received. Range is from 5 to 600 seconds. Default is 15.
local-timezone	(Optional) Uses the local time zone to generate identification fields.
reverse-tunnel private-address	(Optional) Forces a mobile node with a private address to register with reverse tunneling.

Command Default

reg-wait *seconds* : 15

Command Modes

Global configuration

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2(13)T	The **interface-only**, **transmit-only**,and **reverse-tunnel private-address**keywords were added.
12.2(3)XC	The **local-timezone** keyword was added.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

Usage Guidelines

This command enables foreign agent service when at least one care-of address is configured. When no care-of address exists, foreign agent service is disabled.

The foreign agent is responsible for relaying the registration request to the home agent, setting up a tunnel to the home agent, and forwarding packets to the mobile node. The **show** commands used to display relevant information are shown in parentheses in the following paragraph.

When a registration request comes in, the foreign agent will ignore requests when foreign agent service is not enabled on an interface or when no care-of address is advertised. If a security association exists for a visiting mobile node, the visitor is authenticated. The registration bitflag is handled as described in Table 3. The foreign agent checks the validity of the request. If successful, the foreign agent relays the request to the home agent, appending an FH authentication extension if a security association for the home agent exists. The pending registration timer of 15 seconds is started (**show ip mobile visitor pending**command). At most, five outstanding pending requests per mobile node are allowed. If a validity check fails, the foreign agent sends a reply with error code to the mobile node (reply codes are listed in Table 4). A security violation is logged when visiting mobile node authentication fails (**show ip mobile violation**command).

When a registration reply comes in, the home agent is authenticated (**show ip mobile secure home-agent**command) if a security association exists for the home agent (IP source address or home agent address in reply). The reply is relayed to the mobile node.

When registration is accepted, the foreign agent creates or updates the visitor table, which contains the expiration timer. If no binding existed before this registration, a virtual tunnel is created, a host route to the mobile node via the interface (of the incoming request) is added to the routing table (**show ip route mobile**command), and an ARP entry is added to avoid the sendingof ARP requests for the visiting mobile node. Visitor binding is removed (along with its associated host route, tunnel, and ARP entry) when the registration lifetime expires or deregistration is accepted.

When registration is denied, the foreign agent will remove the request from the pending registration table. The table and timers of the visitor will be unaffected.

When a packet destined for the mobile node arrives on the foreign agent, the foreign agent deencapsulates the packet and forwards it out its interface to the visiting mobile node, without sending ARP requests.

The care-of address must be advertised by the foreign agent. This adddress is used by the mobile node to register with the home agent. The foreign agent and home agent use this address as the source and destination point of tunnel, respectively. The foreign agent is not enabled until at least one care-of address is available. The foreign agent will advertise on interfaces configured with the **ip mobile foreign-service**command.

Only care-of addresses with interfaces that are up are considered available.

The **interface-only**and **transmit-only** keywords are used in an aysmmetric link environment, such as satellite communications, where separate uplinks and downlinks exist. The **ip mobile foreign-agent care-of** *interface* **interface-only**commandenables the specified interface to advertise only its own address as the care-of address. All other care-of addresses are not advertised. Other foreign agent interfaces configured for foreign-service will not advertise interface-only care-of addresses. The **ip mobile foreign-agent care-of** *interface* **transmit-only**command informs Mobile IP that the interface acts as an uplink. Registration requests and replies received for this care-of address are treated as transmit-only. This interface will not hear any solicitations. Any care-of address can be configured with the **interface-only** keyword, but only serial interfaces can be configured with the **transmit-only** keyword.

Use the **reverse-tunnel private-address** keywords to force a mobile node with a private address to register with reverse tunnel. Private addresses are IP addresses in the following ranges:

- 10.0.0.0 to 10.255.255.255 (10/8 prefix)
- 172.16.0.0 to 172.31.255.255 (172.16/12 prefix)
- 192.168.0.0 to 192.168.255.255 (192.168/16 prefix)

The table below lists mobile node registration request service bitflags.

Table 1: Mobile Node Registration Request Service Bitflags

Bit Set	**Registration Request**
S	No operation. Not applicable to foreign agent.
B	No operation. Not applicable to foreign agent.
D	Make sure source IP address belongs to the network of the interface.
M	Deny request. Minimum IP encapsulation is not supported.
G	No operation. GRE encapsulation is supported.
r	Sent as zero; ignored on reception. Do not allocate for any other uses.
V	Reserved.
T	Deny if reverse tunneling is disabled on the foreign agent.
reserved	Deny request. Reserved bit must not be set.

The table below lists foreign agent reply codes.

Table 2: Foreign Agent Reply Codes

Code	Reason
64	Reason unspecified.
65	Administratively prohibited.
66	Insufficient resource.
67	Mobile node failed authentication.
68	Home agent failed authentication.
69	Requested lifetime is too long.
70	Poorly formed request.
71	Poorly formed reply.
72	Requested encapsulation is unavailable.
74	Reverse tunnel unsupported.
75	Reverse tunnel is mandatory and T bit is not set.
76	Mobile node too distant.
77	Invalid care-of address.
78	Registration timeout.
79	Delivery style not supported.
80	Home network unreachable (ICMP error received).
81	Home agent host unreachable (ICMP error received).
82	Home agent port unreachable (ICMP error received).
88	Home agent unreachable (other ICMP error received).
98	Missing home agent.
99	Missing home agent address.
100	Unsupported vendor ID or unable to interpret vendor extension type in the registration request extensions sent by the mobile node to the foreign agent.

Code	Reason
101	Unsupported vendor ID or unable to interpret vendor extension type in the registration request extensions sent by the home agent to the foreign agent.
104	Unknown challenge.
105	Missing challenge.
106	Stale challenge.

Examples

The following example enables foreign agent service on Ethernet interface 1, advertising 10.0.0.1 as the care-of address:

```
ip mobile foreign-agent care-of Ethernet0
interface Ethernet0
 ip address 10.0.0.1 255.0.0.0
interface Ethernet1
 ip mobile foreign-service
```

The following example enables foreign agent service on serial interface 4, advertising 10.0.0.2 as the only care-of address. The uplink interface is configured as a transmit-only interface.

```
ip mobile foreign-agent care-of Serial4 interface-only transmit-only
interface Serial4
! Uplink interface
 ip address 10.0.0.2 255.255.255.0
 ip irdp
!
 ip mobile foreign-service
!
```

Related Commands

Command	Description
debug ip mobile advertise	Displays advertisement information.
ip mobile foreign-service	Enables foreign agent service on an interface if care-of addresses are configured.
show ip mobile globals	Displays global information for mobile agents.
show ip mobile interface	Displays advertisement information for interfaces that are providing foreign agent service or are home links for mobile nodes.
show ip mobile secure	Displays mobility security associations for mobile host, mobile visitor, foreign agent, or home agent.
show ip mobile violation	Displays information about security violations.

Command	Description
show ip mobile visitor	Displays the table containing the visitor list of the foreign agent.
show ip route mobile	Displays the current state of the routing table for mobile routes.

ip mobile foreign-agent inject-mobile-networks

To enable direct routing to mobile networks via the foreign agent, use the **ip mobile foreign-agent inject-mobile-networks** command inglobal configuration mode. To disable this functionality, use the **no** form of this command.

ip mobile foreign-agent inject-mobile-networks [**mobnetacl** *access-list-identifier*]

no ip mobile foreign-agent inject-mobile-networks [**mobnetacl** *access-list-identifier*]

Syntax Description

mobnetacl	(Optional) Specifies that the foreign agent can provide direct routing for only the mobile networks covered by the specified access list.
access-list-identifier	(Optional) Name of an access list defined using the **ip access-list** command or number of an access list defined using the **access-list**command.

Command Default

Direct routing via the foreign agent is disabled.

Command Modes

Global configuration

Command History

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

Usage Guidelines

Configure the **ip mobile foreign-agent inject-mobile-networks**command on the foreign agent to enable direct routing.

The value entered for the *access-list-identifier* argument must match the name of an access list defined using the **ip access-list** command or the number of an access list defined using the **access-list**command.

Examples

The following example configures the access list named mobile-net-list and enables direct routing via the foreign agent for mobile networks specified on that access list.

```
ip access-list standard mobile-net-list
 permit any
!
ip mobile foreign-agent inject-mobile-networks mobnetacl mobile-net-list
```

Related Commands

Command	Description
access-list (IP standard)	Defines a standard IP access list.
ip access-list	Defines an IP access list by name.
show ip mobile globals	Displays global information for mobile agents.

ip mobile foreign-service

To enable foreign agent service on if care-of addresses are configured, use the **ip mobile foreign-service**command in interface or global configuration mode. To disable this service, use the no form of this command.

ip mobile foreignservice [**challenge [forwardmfce]** [**timeout** *value*] [**window** *number*]| [**homeaccess** *accesslist*] [**limit** *number*] **[registrationrequired]** [**reversetunnel [mandatory]**]]

no ip mobile foreignservice [**challenge [forwardmfce]** [**timeout** *value*] [**window** *number*]| [**homeaccess** *accesslist*| **limit** *number*| **registrationrequired**| **reversetunnel**]]

Syntax Description

challenge	(Optional) Configures the foreign agent challenge parameters. For releases prior to 12.3T, you cannot use this keyword when you enable foreign agent service on a subinterface.
forward-mfce	(Optional) Enables the foreign agent to forward mobile foreign challenge extensions (MFCEs) and mobile node-AAA extensions to the home agent.
timeout *value*	(Optional) Challenge timeout in seconds. Possible values are from 1 to 10.
window *number*	(Optional) Maximum number of valid challenge values to maintain. Possible values are from 1 to 10. The default is 2.
home-access *access-list*	(Optional) Controls which home agent addresses mobile nodes can be used to register. The access list can be a string or number from 1 to 99. For releases prior to 12.3T, you cannot use this keyword when you enable foreign agent service on a subinterface.
limit *number*	(Optional) Number of visitors allowed on the interface. The Busy (B) bit will be advertised when the number of registered visitors reaches this limit. For releases prior to 12.3T, you cannot use this keyword when you enable foreign agent service on a subinterface.
registration-required	(Optional) Solicits registration from the mobile node even if it uses colocated care-of addresses. The Registration-required (R) bit will be advertised. For releases prior to 12.3T, you cannot use this keyword when you enable foreign agent service on a subinterface.

reverse-tunnel [**mandatory**]	(Optional) Enables reverse tunneling on the foreign agent. For releases prior to 12.3T, you cannot use this keyword when you enable foreign agent service on a subinterface.

Command Default

Foreign agent service is not enabled. There is no limit to the number of visitors allowed on an interface.**window** *number:* 2 Foreign agent reverse tunneling is not enabled. When foreign agent reverse tunneling is enabled, it is not mandatory by default.

Command Modes

Interface and global configuration

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.1(3)XS	The **challenge** keyword and associated parameters were added.
12.2(2)XC	The **reverse-tunnel**[**mandatory**]keywords were added.
12.2(13)T	The **challenge** keyword and associated parameters and the **reverse-tunnel**[**mandatory**]keywords were integrated into Cisco IOS Release 12.2(13)T.
12.3(11)T	Global configuration mode was added.

Usage Guidelines

This command enables foreign agent service on the interface or all interfaces (global configuration). The foreign agent (F) bit will be set in the agent advertisement, which is appended to the IRDP router advertisement whenever the foreign agent or home agent service is enabled on the interface.

Note The Registration-required bit only tells the visiting mobile node to register even if the visiting mobile node is using a colocated care-of address. You must set up packet filters to enforce this. For example, you could deny packets destined for port 434 from the interface of this foreign agent.

When you use the **reverse-tunnel** keyword to enable foreign agent reverse tunneling on an interface, the reverse tunneling support (T) bit is set in the agent advertisement.

Cisco Express Forwarding (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, then there is no need to disable CEF at the global configuration level.

Below table lists the advertised bitflags.

Table 3: Foreign Agent Advertisement Bitflags

Bit Set	Service Advertisement
T	Set if the **reverse-tunnel** parameter is enabled.
R	Set if the **registration-required** parameter is enabled.
B	Set if the number of visitors reached the **limit** parameter.
H	Set if the interface is the home link to the mobile host (group).
F	Set if foreign-agent service is enabled.
M	Never set.
G	Always set.
V	Reserved.
reserved	Never set.

Examples

The following example shows how to enable foreign agent service for up to 100 visitors:

```
interface Ethernet 0
 ip mobile foreign-service limit 100 registration-required
```

The following example shows how to enable foreign agent reverse tunneling:

```
interface ethernet 0
 ip mobile foreign-service reverse-tunnel
```

The following example shows how to configure foreign agent challenge parameters:

```
interface ethernet 0
 ip mobile foreign-service challenge window 2
```

Related Commands

Command	Description
ip cef	Enables CEF on the RP card.
ip mobile tunnel	Specifies the settings of tunnels created by Mobile IP.
show ip mobile interface	Displays advertisement information for interfaces that are providing foreign agent service or are home links for mobile nodes.

ip mobile home-agent

To enable and control home agent (HA) services, use the **ip mobile home-agent** command in global configuration mode. To disable these services, use the **no** form of this command.

ip mobile homeagent [**address** *ip-address*] **[broadcast]** [**care-of-access** *access-list*] [**lifetime** *seconds*] **[nat-detect]** [**replay** *seconds*] [**reverse-tunnel** {**off**| **private-address**}] [**roam-access** *access-list*] **[strip-realm]** **[suppress-unreachable]** **[local-timezone]** [**unknown-ha** [**accept [reply]**| **deny**]] **[send-mn-address]**

no ip mobile home-agent [**address** *ip-address*] **[broadcast]** [**care-of-access** *accessl-ist*] [**lifetime** *seconds*] **[nat-detect]** [**replay** *seconds*] [**reverse-tunnel** {**off**| **private-address**}] [**roam-access** *access-list*] **[strip-realm]** **[suppress-unreachable]** **[local-time-zone]** [**unknown-ha** [**accept [reply]**| **deny**]] **[send-mn-address]**

Syntax Description

address *ip-address*	(Optional) Specifies the IP address of the HA. **Note** This option is only applicable when HA redundancy is used for virtual networks.
broadcast	(Optional) Enables forwarding of broadcast datagrams to the mobile node (MN). By default, broadcasting is disabled.
care-of-access *access-list*	(Optional) Controls which care-of addresses (CoAs) in registration requests are permitted by the HA. By default, all CoAs are permitted. The access-list argument can be a string or number from 1 to 99.
lifetime *seconds*	(Optional) Specifies the global registration lifetime for an MN in seconds. Range is from 3 to 65535 (infinity). Default is 36000 (10 hours). **Note** This configuration can be overridden by the individual MN configuration. Registrations requesting a lifetime greater than this value will still be accepted, but will use this lifetime value.
nat-detect	(Optional) Allows the HA to detect registration requests from a MN traversing a Network Address Translation (NAT)-enabled device and apply a tunnel to reach the MN. By default, NAT detection is disabled.
replay *seconds*	(Optional) Sets the replay protection time-stamp value in seconds. A registration received within the router clock time plus or minus 7 is valid.

reverse-tunnel off | private-address	(Optional) Enables support of reverse tunnel by the HA. By default, reverse tunnel support is enabled. The keywords are as follows: • off--Disables support of reverse tunnel. • private-address--Reverse tunnel mandatory for private Mobile IP addresses.
roam-access *access - list*	(Optional) Controls which MNs are permitted or denied to roam. By default, all specified MNs can roam.
strip-realm	(Optional) Strips the realm part of the Network access identifier (NAI) before authentication is performed. This option is useful if the majority of MNs have the identical realm, for example, in the case of enterprise networks.
suppress-unreachable	(Optional) Disables sending Internet Control Message Protocol (ICMP) unreachable messages to the source when an MN on the virtual network is not registered. By default, ICMP unreachable messages are sent.
local-timezone	(Optional) Uses the local time zone to generate identification fields.
unknown-ha [**accept** [**reply**] | **deny**	Accepts or denies an unknown HA registration request. The keywords are as follows: • accept--(Optional) HA accepts the registration request with an HA address different from the IP destination of the registration request. The HA address set in the registration reply is that of the IP destination address. • reply--(Optional) HA uses the received HA address in reply. • deny--(Optional) HA denies the registration request with an HA address different from the IP destination of the registration request with error code Unknown HomeAgent. The HA address set in the reject registration reply is that of the IP destination address. **Note** This command option can be used in a testing environment when the home agent is in private addressing space behind a NAT gateway.

send-mn-address	Sends the home address as received in the registration request and in the access request messages for the HA Challenge Handshake Authentication Protocol (CHAP). **Note** You must configure this keyword in the HA to send radius-server vsa send authentication 3gpp2 attributes. This keyword is available only on PDSN platforms running specific PDSN code images.

Command Default

The command is disabled. Broadcasting is disabled. Reverse tunnel support is enabled. ICMP unreachable messages are sent. NAT detection is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2(2)XC	The **strip-nai-realm** and **local-timezone** keywords were added.
12.2(13)T	The **nat-detect** keyword was added.
12.3(4)T	The **unknown-ha**, **accept**, **reply**, **deny** and **send-mn-address** keywords were added.

Usage Guidelines

This command enables and controls HA services on a router. Changes to service take effect immediately; however, broadcast and lifetime settings for previously registered MNs are unaffected. Tunnels are shared by MNs registered with the same endpoints, so the **reverse-tunnel-off** keyword also affects registered MNs.

The HA processes registration requests from the MN and sets up tunnels and routes to the CoA. Packets to the MN are forwarded to the visited network.

The HA will forward broadcast packets to MNs if the MNs are registered with the service. However, heavy broadcast traffic uses the CPU of the router.

The HA can control where the MNs roam by the **care-of-access** keyword, and which MN is allowed to roam by the **roam-access** keyword.

When a registration request comes in, the HA ignores requests when HA service is not enabled or the security association of the MN is not configured. The latter condition occurs because the security association must be available for the MH authentication extension in the reply. If a security association exists for the FA (IP source address or CoA in the request), the FA is authenticated, and then the MN is authenticated. The Identification field is verified to protect against replay attack. The HA checks the validity of the request (see Table 3) and sends a reply. (Reply codes are listed in Table 4.) A security violation is logged when FA authentication, MH authentication, or identification verification fails. (The violation reasons are listed in Table 5.)

After registration is accepted, the HA creates or updates the mobility binding of the MN, which contains the expiration timer. If no binding existed before this registration, a virtual tunnel is created, a host route to the MN via the care-of address is added to the routing table, and gratuitous ARPs are sent out. For deregistration, the host route is removed from the routing table, the virtual tunnel interface is removed (if no MNs are using it), and gratuitous ARP messages are sent out if the MN is back home. Mobility binding is removed (along with its associated host route and tunnel) when registration lifetime expires or deregistration is accepted.

By default, the HA uses the entire NAI string as the username for authentication (which may be with local security association or retrieved from the AAA server). The strip-nai-realm keyword instructs the HA to strip off the realm part of NAI (if it exists) before performing authentication. Basically, the MN is identified by only the user name part of the NAI. This option is useful if the majority of MNs belong to the same realm, for example, in the case of enterprise networks.

When the packet destined for the MN arrives on the HA, the HA encapsulates the packet and tunnels it to the care-of address. If the Don’t Fragment (DF) bit is set in the packet via the **ip mobile tunnel path-mtu-discovery** global configuration command, the HA will copy the DF bit from the original packet to the new tunnel IP header. This allows the path MTU discovery to set the MTU of the tunnel. Subsequent packets greater than the MTU of the tunnel will be dropped and an ICMP datagram too big message will be sent to the source (correspondent node). If the HA loses the route to the tunnel endpoint, the host route to the MN will be removed from the routing table until the tunnel route is available. Packets destined for the MN without a host route will be sent out the interface (home network) or to the virtual network (see the description of the **suppress-unreachable** keyword). For subnet-directed broadcasts to the home link, the HA will send a copy to all MNs registered with the broadcast routing option.

Some companies block ICMP datagram too big messages. If the message does not reach the original correspondent node sending the packet, the correspondent node will simply resend the same size packet. To work around this problem, turn off Path MTU Discovery with the **no ip mobile tunnel path-mtu-discovery** command. The DF bit will not be copied from the original packet and the tunnel packet can be fragmented.

The **ip mobile home-agent nat-detect** option is supported for MNs using a collocated care-of address and registering through the FA. The MN will use the NAT inside address as the collocated care-of address used in its registration requests. If a MN is using a FA CoA address, the MN can be detected behind a NAT gateway.

The **ip mobile home-agent unknown-ha**option can be useful in a testing environment when the HA is using a private address behind a NAT gateway. A MN would need to access the HA through the NAT box while it is on a public network domain. However, NAT will translate the destination IP address of the registration request to the private address of the HA. When the HA checks the HA field in the registration request, it does not match one of the interfaces. The packet can not be processed properly and the tunnels are not set up properly. The **ip mobile home-agent unknown-ha** command allows the HA to accept the unknown (translated) address and process the registration request.

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

The MN requests services from the HA by setting bits in the registration request. The table below shows the services the MN can request.

Table 4: HA Registration Bitflags

Bit Set	Definition
S	Accept with code 1 (no simultaneous binding).
B	Accept. Broadcast can be enabled or disabled.

Bit Set	Definition
D	Accept. Tunnel endpoint is a colocated care-of address.
M	Deny. Minimum IP encapsulation is not supported.
G	Accept. GRE encapsulation is supported.
V	Deny if this bit is set.
T	Accept if the **reverse-tunnel-off** parameter is not set.
reserved	Deny. Reserved bit must not be set.

The table below lists the HA registration reply codes. The codes tell the MN whether the registration was accepted or denied. If registration is denied, the reply code gives the reason.

Table 5: HA Registration Reply Codes

Code	Reason
0	Accept.
1	Accept. No simultaneous bindings.
128	Reason unspecified.
129	Administratively prohibited.
130	Insufficient resource.
131	MN failed authentication.
132	FA failed authentication.
133	Registration identification mismatched (timestamp is off).
134	Poorly formed request.
136	Unknown HA address.
137	Reverse tunnel is unavailable.
138	Reverse tunnel is mandatory and T bit not set.
139	Unsupported encapsulation.

Code	Reason
140	Unsupported vendor id or unable to interpret registration request extensions sent by the MN to the home agent.
141	Unsupported vendor id or unable to interpret registration request extensions sent by the FA to the home agent.
142	Active home agent failed authentication.

Below table lists security violation codes.

Table 6: Security Violation Codes

Code	Reason
1	No mobility security association.
2	Bad authenticator.
3	Bad identifier.
4	Bad SPI.
5	Missing security extension.
6	Other.
7	Stale request.

Examples

The following example enables broadcast routing and specifies a global registration lifetime of 7200 seconds (2 hours):

```
ip mobile home-agent broadcast lifetime 7200
```

Related Commands

Command	Description
ip mobile tunnel	Specifies the setting of tunnels created by Mobile IP.
show ip mobile binding	Displays the mobility binding table.
show ip mobile globals	Displays global information for mobile agents.

ip mobile home-agent aaa user-password

To configure an authentication password for the downloading of security associations from a AAA server, use the **ip mobile home-agent aaa user-password** command in global configuration mode. To remove the password requirement, use the **no**form of this command.

ip mobile home-agent aaa user-password {**0** *password*| **7** *encrypted-password*| *password*}

no ip mobile home-agent aaa user-password

Syntax Description

0 *password*	Specifies that an unencrypted password will follow. The unencrypted (cleartext) password.
7 *password*	Specifies that an encrypted password will follow. The encrypted password.
password	The unencrypted (cleartext) password.

Command Default

The default password is cisco.

Command Modes

Global configuration

Command History

Release	Modification
12.3	This command was introduced.

Usage Guidelines

When a mobile node sends a registration request packet to the home agent, Mobile IP requires a security association for registration authentication. Security associations for a mobile node can be configured on the home agent or retrieved by the home agent from a AAA server.

If security associations are retrieved from a AAA server, the AAA access-request packets used to retrieve the security associations require a challenge and response. If the registration request of the mobile node does not contain a challenge and response, the home agent auto-generates a challenge and creates a response using the default password “cisco” unless you specify a different password using the **ip mobile home-agent aaa user-password** command. In either case, a single password is used for all mobile nodes.

The AAA server will read the challenge in the access-request packet of the mobile node, and using the password of the mobile node that is stored on the AAA server, create the response to the challenge. It then authenticates the mobile node, identified by its IP address (or network access identifier), by comparing the two responses to ensure they are identical. For this reason, the password configured by the **ip mobile home-agent aaa user-password** command must match the user password in the user profile on the AAA server.

Mobile nodes that include a challenge and response in their registration request, such as in the case of dynamic security association and key distribution, do not use the defined password. Instead, the home agent copies the challenge/response from the registration request into the AAA access-request packet. Thus, a mobile node in this scenario can have a “unique” password.

You can enable or disable password encryption with the **service password-encryption** command. If thiscommand is enabled, even if the **ip mobile home-agent aaa user-password 0** *password is used, the password will be encrypted.*

Examples

The following example enables the encrypted password “ $1$i5Rkls3L0yxzS8t9” for authenticating the downloading of security associations from the AAA server:

```
ip mobile home-agent aaa user-password 7 $1$i5Rkls3L0yxzS8t9
```

The following example enables the unencrypted password “ pswd2” for authenticating the downloading of security associations from the AAA server:

```
ip mobile home-agent aaa user-password 0 pwsd2
```

The following example enables the unencrypted password “ pswdmobile” for authenticating the downloading of security associations from the AAA server:

```
ip mobile home-agent aaa user-password pswdmobile
```

Related Commands

Command	Description
service password-encryption	Encrypts passwords.

ip mobile home-agent accounting

To enable home agent accounting services on the router, use the **ip mobile home-agent accounting** command in global configuration mode. To disable these services, use the **no** form of this command.

ip mobile home-agent accounting {**default**| *list-name*}

no ip mobile home-agent accounting {**default**| *list-name*}

Syntax Description

default	Uses the listed accounting methods that follow this argument as the default list of methods for accounting services.
list-name	Character string used to name the list of at least one of the accounting methods.

Command Default

The command is disabled.

Command Modes

Global configuration

Command History

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

Usage Guidelines

This command enables and controls home agent accounting services on the router. First, use the **aaa accounting** global configuration command to define the accounting method list. Next, apply the same accounting method list on the home agent using the **ip mobile home-agent accounting** global configuration command.

Examples

The following example enables home agent accounting for the list named mobile-list:

```
ip mobile home-agent accounting mobile-list
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes.

ip mobile home-agent dynamic-address

To set the home agent address field in a Registration Response packet, use the ip mobile home-agent dynamic-address command in global configuration. To disable this functionality, or to reset the field use the **no** form of this command.

ip mobile home-agent dynamic-address *ip-address*

no ip mobile home-agent dynamic-address *ip-address*

Syntax Description

ip-address	The IP address of the Home Agent.

Command Default

The Home Agent Address field will be set to the values specified by the ip-address argument.

Command Modes

Global configuration

Command History

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

Examples

In the following example, the dynamic home-agent address is set to 10.1.1.1:

```
Router# ip mobile home-agent dynamic-address 10.1.1.1
```

ip mobile home-agent multi-path

To enable the home agent to process registration requests with multiple path support for all mobile routers, use the **ip mobile home-agent multi-path**command in global configuration mode. To disable multipath support on the home agent, use the **no** form of this command.

ip mobile home-agent multi-path [**metric** {**bandwidth**| **hopcount**}]

no ip mobile home-agent multi-path [**metric** {**bandwidth**| **hopcount**}]

Related Commands

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 enabled by default on the mobile router.

Command Modes

Global 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. The **multi-path** command in mobile networks configuration mode overrides the global setting.

Examples

The following example shows how to configure the home agent to globally process registration requests for all mobile routers:

```
!
router mobile
exit
ip mobile home-agent multi-path
```

Related Commands

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

ip mobile home-agent nat traversal

To enable NAT traversal support for Mobile IP home agents (HAs), use the **ip mobile home-agent nat traversal** command in global configuration mode. To disable Network Address Translation (NAT) traversal support for Mobile IP for the HA, use the **no** form of this command.

ip mobile home-agent nat traversal [**keepalive** *keepalive-time*] [**forced** {**accept**| **reject**}]

no ip mobile home-agent nat traversal [**keepalive** *keepalive-time*] [**forced** {**accept**| **reject**}]

Syntax Description

keepalive *keepalive-time*	(Optional) Configures the keepalive interval in seconds the HA uses in registration replies. When the HA replies with a keepalive interval other than zero, it forces the FA or MN to use this interval. If it replies with an interval of zero, the FA or MN should use its default configured interval. The range is 0 to 65535 seconds. The default is 110 seconds.
forced	(Optional) Enables the HA to accept or reject forced UDP tunneling from the mobile node (MN) regardless of the NAT-detection outcome. **accept** --Accepts UDP tunneling. **reject** --Rejects UDP tunneling. If the **forced** keyword is not specified, the command defaults to rejecting registration requests where the “force” bit is set in the UDP tunnel extension. MN registration attempts will fail until the MN retries without the “forced” bit set in the UDP tunnel extension. The registration will fail until the MN retries the registration.

Command Default

NAT traversal support for Mobile IP is disabled for the HA.

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.4T	the **keepalive** *keepalive-time*range changed.

Usage Guidelines

Enable this command if your MNs will roam behind a NAT-enabled router or firewall.

Examples

The following example shows an HA configured with a keepalive timer set to 56 seconds and forced to accept UDP tunneling.

```
ip mobile home-agent nat traversal 56 forced accept
ip mobile home-agent replay 255
ip mobile home-agent redundancy Phy1 virtual-network
```

Related Commands

Command	Description
debug ip mobile	Displays IP mobility activities.
ip mobile foreign-agent nat traversal	Enables NAT UDP traversal support for MIP FAs.
show ip mobile binding	Displays the mobility binding table.
show ip mobile globals	Displays global information about MIP HAs, FAs, and MNs.
show ip mobile tunnel	Displays information about UDP tunneling.
show ip mobile visitor	Displays the table that contains a visitor list of FAs.

ip mobile home-agent redundancy

To configure the home agent for redundancy by using the Hot Standby Router Protocol (HSRP) group name, use the **ip mobile home-agent redundancy** command in global configuration mode. To remove the address, use the **no** form of this command.

ip mobile home-agent redundancy *hsrp-group-name* [**[virtual-network] address address**] [**mode active-standby**] **[swact-notification]**

no ip mobile home-agent redundancy *hsrp-group-name* [**[virtual-network] address address**] [**mode active-standby**] **[swact-notification]**

Syntax Description

hsrp-group-name	Specifies the HSRP group name.
virtual-network	(Optional) Specifies that the HSRP group is used to support virtual networks.
address *address*	(Optional) Home agent address.
mode active-standby	(Optional) Allows the bindings to come up (with local pool addressing for virtual-networks) with the home agent IP address specified under the loopback interface.
swact-notification	(Optional) Notifies the RADIUS server of a home agent failover.

Command Default

No global home agent addresses are specified.

Command Modes

Global configuration

Command History

Release	Modification
12.0(2)T	This command was introduced.
12.2(8)T	The command changed from **ip mobile home-agent standby** to **ip mobile home-agent redundancy**.
12.4(11)T	The **mode active-standby** and **swact-notification** keywords were added.

Usage Guidelines

The **virtual-network** keyword specifies that the HSRP group supports virtual networks.

Note Redundant home agents must have identical Mobile IP configurations. You can use a standby group to provide HA redundancy for either physical or virtual networks, but not both at the same time.

When Mobile IP standby is configured, the home agent can request mobility bindings from the peer home agent. When Mobile IP standby is deconfigured, the home agent can remove mobility bindings. Operation of home agent redundancy on physical and virtual networks is described as follows:

- **Physical network** --Only the active home agent will receive registrations on a physical network. It updates the standby home agent. The standby home agent requests the mobility binding table from the active home agent. When Mobile IP standby is deconfigured, the standby home agent removes all bindings, but the active home agent keeps all bindings.
- **Virtual network** --Both active and standby home agents receive registrations if the loopback interface is used; each will update the peer after accepting a registration. Otherwise, the active home agent receives registrations. Both active and standby home agents request mobility binding tables from each other. When Mobile IP standby is deconfigured, the standby or active home agent removes all bindings.

Note The **swact-notification** option notifies the RADIUS server of a home agent failover. This is achieved by including the cisco-avpair radius attribute “mobileip-rfswat=1” in RADIUS accounting records. This attribute is included only in the first accounting record of a binding generated after a failover, and if that binding was created before the failover.

Examples

The following example specifies an HSRP group named SanJoseHA:

```
ip mobile home-agent redundancy SanJoseHA
```

Related Commands

Command	Description
show ip mobile globals	Displays global information for mobile agents.

ip mobile home-agent redundancy periodic-sync

To synchronize the byte and packet counters for each binding to the standby unit using an accounting update event, use the ip mobile home-agent redundancy periodic-sync command in global configuration mode. To disable this functionality, use the no form of this command.

ip mobile home-agent redundancy *hsrp-group-name* [**[virtual-network] address address**] **periodic-sync**

no ip mobile home-agent redundancy *hsrp-group-name* [**[virtual-network] address address**] **periodic-sync**

Syntax Description

hsrp-group-name	Specifies the HSRP group name.
virtual-network	(Optional) Specifies that the HSRP group is used to support virtual networks.
address address	(Optional) Home agent address.

Command Default

There are no default values for this command.

Command Modes

Global configuration

Command History

Release	Modification
12.3(14)YX	This command was introduced.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.

Usage Guidelines

The byte and packet counters for each binding are synchronized to the standby unit using an accounting update event only if the byte counts have changed since the last synchronization.

Examples

In the following example, the byte and packet counters for each binding will be periodically synchronized between the active and standby unit:

```
Router# ip mobile home-agent redundancy group1 periodic-sync
```

ip mobile home-agent reject-static-addr

To configure the HA to reject Registration Requests from MNs under certain conditions, use the ip mobile home-agent reject-static-addr sub-command under the ip mobile home-agent global configuration command.

ip mobile home-agent reject-static-addr

Syntax Description

This command has not arguments or keywords

Command Modes

Sub-command of the ip mobile home-agent global configuration command.

Command History

Release	Modification
12.2(8)BY	This command was introduced.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.

Usage Guidelines

You must first configure the ip mobile home-agent command to use this sub-command.

If an MN that has a binding to the HA with a static address tries to register with the same static address again, then the HA rejects the second RRQ from the MN.

Examples

The following example illustrates the ip mobile home-agent reject-static-addr command:

```
Router# ip mobile home-agent reject-static-addr
```

ip mobile home-agent resync-sa

To configure the home agent to clear out the old cached security associations and requery the AAA server for a new security association when the mobile node fails authentication, use the **ip mobile home-agent resync-sa** command in global configuration mode. To disable this functionality, use the **no** form of this command.

ip mobile home-agent resync-sa *seconds*

no ip mobile home-agent resync-sa *seconds*

Syntax Description

seconds	Specifies the time in which the home agent will wait to initiate a resynchronization.

Command Default

This command is off by default. The normal behavior of the home agent is to never requery the AAA server for a new security association.

Command Modes

Global configuration

Command History

Release	Modification
12.2	This command was introduced.

Usage Guidelines

You must enable security association caching for the **ip mobile home-agent resync-sa** command to work. Use the **ip mobile host** aaa load-sa global configuration command to enable caching of security associations retrieved from a AAA server.

When a security association is downloaded for a mobile node from a AAA server, the security association is time stamped. If the mobile node fails reregistration and the time interval since the security association was cached is greater than *sec* seconds, the home agent will clear out the old security association and requery the AAA server. If the time period is less than the *sec* value, the home agent will not requery the AAA server for the security association of the mobile node.

The *sec* value represents the number of seconds the home agent will consider the downloaded security association synchronized with the AAA server. After that time period, it is considered old and can be replaced by a new security association from the AAA server.

This time-based resynchronization process helps prevent denial-of-service attacks on the AAA server and provides a way to synchronize the home agent's cached security association entry when a change to the security association for the mobile node is made at the AAA server and on the mobile node. By using this process, once the mobile node fails reregistration with the old cached security association, the home agent will clear the cache for that mobile node, and resynchronize with the AAA server.

Examples

In the following example, if a registration fails authentication, the home agent retrieves a new security association from the AAA server if the existing security association was downloaded more than 10 seconds ago:

```
ip mobile home-agent resync-sa 10
```

Related Commands

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

ip mobile home-agent revocation

To enable support for MIPv4 registration revocation on the home agent, use the ip mobile home-agent revocation command in global configuration mode. To disable support for registration revocation, use the no form of the command.

ip mobile home-agent revocation [**timeout seconds**] [**retransmit retries**] [**timestamp msec**]

no ip mobile home-agent revocation [**timeout seconds**] [**retransmit retries**] [**timestamp msec**]

Syntax Description

timeout seconds	(Optional) Configures the time interval (in seconds) between retransmission of MIPv4 registration revocation message. The no version restores the time interval between retransmission of MIPv4 registration revocation Message to the default value. The default is 3 seconds. The range is from 1 to 100 seconds
retransmit retries	(Optional) Configures the number of times MIPv4 registration revocation messages are retransmitted. The no version of this command restores the retransmit number to the default value. The default is 3 retransmissions. The range is from 1 to 100 retransmissions.
timestamp msec	(Optional) Configures the units in which the timestamp value in the revocation support extension and revocation message should be encoded. By default the timestamp value will be sent as seconds. If the msec option is specified, the values will be encoded in milliseconds.

Command Default

The home agent does not support registration revocation.

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.

Examples

In the following example, the MIPv4 registration message will be retransmitted a maximum of 5 times with a time interval of 4 seconds in between retransmissions:

```
Router(config)#ip mobile home-agent revocation timeout 4 retransmit 5
```

ip mobile home-agent template tunnel

To configure a home agent to use the template tunnel, use the ip mobile home-agent template tunnel command in global configuration. To disable the use of the template tunnel, use the no form of the command.

ip mobile home-agent template tunnel interface-id address ha-address

no ip mobile home-agent template tunnel interface-id address ha-address

Syntax Description

interface-id	Specifies the template tunnel interface ID from which to apply ACLs.
address ha-address	Specifies the home agent address. ACLs will be applied to tunnels with ha-address as the local end point.

Command Default

The home agent does not use a template tunnel.

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)XJW	This command was introduced.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.

Examples

In the following example, the home agent is configured to use the template tunnel:

```
Router(config)# interface tunnel 10
!
Router(config)# ip mobile home-agent template tunnel 10 address 10.0.0.1
```

ip mobile host

To configure the mobile host or mobile node group, use the **ip mobile host** command in global configuration mode. To disable these services, use the **no** form of this command.

ip mobile host {*lower* [*upper*]| **nai** *string* [**static-address** {*addr1* [*addr2*] [*addr3*] [*addr4*] [*addr5*]| **local-pool**- *name*}] [**address** {*addr*| **pool** {**local** *name*| **dhcp-proxy-client** [**dhcp-server** *addr*]}}] {**interface** *name*| **virtual-network** *networkaddress mask*} [**aaa** [**load-sa [permanent]**]] [**authorized-pool** *name*] **[skip-aaa-reauthentication]** [**care-of-access** *access-list*] [**lifetime** *seconds*]}

no ip mobile host {*lower* [*upper*]| **nai** *string* [**static-address** {*addr1* [*addr2*] [*addr3*] [*addr4*] [*addr5*]| **local-pool** *name*}] [**address** {*addr*| **pool** {**local** *name*| **dhcp-proxy-client** [**dhcp-server** *addr*]}}] {**interface** *name*| **virtual-network** *networkaddress mask*} [**aaa** [**loadsa [permanent]**]] [**authorized-pool** *name*] **[skip-aaa-reauthentication]** [**care-of-access** *accesslist*] [**lifetime** *seconds*]}

Syntax Description

lower upper	One or a range of mobile host or mobile node group IP addresses. The upper end of the range is optional.
nai *string*	Network access identifier. The NAI can be a unique identifier (username@realm) or a group identifier (@realm).
static-address	(Optional) Indicates that a static IP address is to be assigned to the flows on this NAI. This parameter is not valid if the NAI is a realm.
addr1, addr2, ...	(Optional) One to a maximum of five IP addresses to be assigned using the static-address keyword.
local-pool *nam* e	(Optional) Name of the local pool of addresses to use for assigning a static IP address to this NAI.
address	(Optional) Indicates that a dynamic IP address is to be assigned to the flows on this NAI.
addr	(Optional) IP address to be assigned using the address keyword.
pool	(Optional) Indicates that a pool of addresses is to be used in assigning a dynamic IP address.
local *name*	(Optional) The name of the local pool to use in assigning addresses.
dhcp-proxy-client	(Optional) Indicates that the DHCP request should be sent to a DHCP server on behalf of the mobile node.

dhcp-server *addr*	(Optional) IP address of the DHCP server.
interface *name*	When used with DHCP, specifies the gateway address from which the DHCP server should select the address.
virtual-network *network-address mask*	Indicates that the mobile station resides in the specified virtual network, which was created using the **ip mobile virtual-network** command.
aaa	(Optional) Retrieves security associations from a AAA (TACACS+ or RADIUS) server. Allows the home agent to download address configuration details from the AAA server.
load-sa	(Optional) Caches security associations after retrieval by loading the security association into RAM. See the table Caching Behavior for Security Associations for details on how security associations are cached for NAI hosts and non-NAI hosts.
permanent	(Optional) Caches security associations in memory after retrieval permanently. Use this optional keyword only for NAI hosts.
authorized-pool *name*	(Optional) Verifies the IP address assigned to the mobile node if it is within the pool specified by the name argument.
skip-aaa-reauthentication	(Optional) When configured, the home agent does not send an access request for authentication for mobile IP re-registration requests. When disabled, the home agent sends an access request for all Mobile IP registration requests.
care-of-access *access-list*	(Optional) Access list. This can be a named access list or standard access list. The range is from 1 to 99. Controls where mobile nodes roam--the acceptable care-of addresses.
lifetime *seconds*	(Optional) Lifetime (in seconds). The lifetime for each mobile node (group) can be set to override the global value. The range is from 3 to 65535 (infinite).

Command Default

No host is configured.

Command Modes

Global configuration

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2(2)XC	The **nai** keyword and associated parameters were added.
12.2(13)T	The **permanent** keyword was added and the command was integrated into Cisco IOS Release 12.2(13)T.
12.3(4)T	The **authorized-pool** *and* **skip-aaa-reauthentication**keywordswere added.

Usage Guidelines

This command configures the mobile host or mobile node group (ranging from *lower* address to *upper* address) to be supported by the home agent. These mobile nodes belong to the network on an interface or a virtual network (via the **ip mobile virtual-network** command). The security association for each mobile host must be configured using the **ip mobile secure** command or downloaded from a AAA server.

All hosts must have security associations for registration authentication. Mobile nodes can have more than one security association. The memory consumption calculations shown in the first table below are based on the assumption of one security association per mobile node. Caching behavior of security associations differs between NAI and non-NAI hosts as described in the second table below.

The nai keyword allows you to specify a particular mobile node or range of mobile nodes. The mobile node can request a static IP address (static-address keyword), which is configured using the addr1 variable (for a specific address) or the local-pool keyword (for an IP address from an address pool; the requested address must be in the pool). Or, the mobile node can request a dynamic address (address keyword), which is configured using the addr variable (for a specific address) or the pool keyword (for an IP address from a pool or DHCP server). If this command is used with the Packet Data Serving Node (PDSN) proxy Mobile IP feature and a realm is specified in the ip mobile proxy-host nai command, then only a pool of addresses can be specified in this command.

The address pool can be defined by a local pool or by use of a DHCP proxy client. For DHCP, the interface name keyword and argument combination specifies the gateway address from which the DHCP server should select the address and the dhcp-server keyword specifies the DHCP server address. The NAI is sent in the client-id option of the DHCP packet and can be used to provide dynamic DNS services.

You can also use this command to configure the static IP address or address pool for multiple flows with the same NAI. A flow is a set of {NAI, IP address}.

Security associations can be stored by using one of three methods:

- On the router
- On the AAA server, retrieve security association each time registration comes in (**aaa** optional keyword)
- On the AAA server, retrieve and cache security association (**aaa load-sa**option)

Each method has advantages and disadvantages, which are described in the table below.

Table 7: Methods for Storing Security Associations

Storage Method	Advantage	Disadvantage
On the router	• Security association is in router memory, resulting in fast lookup. • For home agents supporting fewer than 1500 mobile nodes, this provides optimum authentication performance and security (keys never leave router).	• NVRAM of router is limited, cannot store many security associations. Each security association configuration takes about 80 bytes. For 125 KB NVRAM, you can store about 1500 security associations on a home agent.
On the AAA server, retrieve security association each time registration comes in	• Central administration and storage of security association on AAA server. • If keys change constantly, administration is simplified to one server, latest keys always retrieved during registration. • Router memory (DRAM) is conserved. Router will need memory only to load in a security association, and then release the memory when done.	• Requires network to retrieve security association, slower than other storage methods, and dependent on network and server performance. • Multiple home agents that use one AAA server, which can become the bottleneck, can get slow response. • Key can be snooped if packets used to retrieve from AAA are not encrypted (for example, using RADIUS or unencrypted TACACS+ mode).
On the AAA server, retrieve and store security association	• AAA acts as an offload configuration server, security associations are loaded into router DRAM, which is more abundant (for example, 16 MB, 32 MB, 64 MB) when the first registration comes in. Each security association takes only about 50 bytes of DRAM, so 10,000 mobile nodes will use up 0.5 MB. • If keys remain fairly constant, once security associations are loaded, home agent authenticates as fast as when stored on the router. • Only security associations that are needed are loaded into router memory. Mobile nodes that never register will not waste memory.	• If keys change on the AAA server after the mobile node registered, then you need to use **clear ip mobile secure**command to clear and load in new security association from AAA, otherwise the security association of the router is stale.

The caching behavior of security associations for NAI hosts and non-NAI hosts is described in in the below table.

Table 8: Caching Behavior for Security Associations

Keyword Option	NAI Hosts	Non-NAI Hosts
aaa	Security associations are deleted after authentication and are not cached.	Security associations are deleted after authentication and are not cached.
aaa load-sa	The security association is cached while the mobile node is registered. If the mobile node’s registration is deleted, the security association is removed.	Security associations are cached permanently.
aaa load-sa permanent	Security associations are cached permanently after being retrieved from the AAA server.	--

Note On the Mobile Wireless Home Agent, the following conditions apply: If the aaa load-sa option is configured, the Home Agent caches the SA locally on first registration. In this case the Home Agent will not invoke the RADIUS authorization procedure for re-registration. If aaa load-sa skip-aaa-reauthentication is configured, the Home Agent caches the SA locally on first registration; however, the Home Agent will not invoke HA-CHAP procedure for re-registration. The aaa load-sa permanent option is not supported on the Mobile Wireless Home Agent, and should not be configured.

Examples

The following example configures a mobile node group to reside on virtual network 20.0.0.0 and retrieve mobile node security associations from a AAA server every time the mobile node registers:

```
ip mobile host 20.0.0.1 20.0.0.3 virtual-network 20.0.0.0 aaa
```

The following example configures a mobile node group to reside on virtual network 10.99.1.0 and retrieve and cache mobile node security associations from a AAA server. The cached security association is then used for subsequent registrations.

```
ip mobile host 10.99.1.1 10.99.1.100 virtual-network 10.99.1.0 aaa load-sa
```

The following example configures a local pool of dynamic addresses to be used in assigning IP addresses to mobile nodes in the cisco.com domain:

```
ip mobile host nai @cisco.com address pool local mobilenodes virtual-network 9.0.0.0 255.0.0.0
 aaa lifetime 180
```

The following example configures a local pool of dynamic addresses to be used in assigning IP addresses to mobile nodes in the cisco.com domain. The security associations that are retrieved from the AAA server are cached as long as the binding is present and are deleted on the home agent when the binding is removed (due to manual clearing of the binding or lifetime expiration).

```
ip mobile host nai @cisco.com address pool local mobilenodes virtual-network 10.2.0.0
255.255.0.0 aaa load-sa lifetime 180
```

The following example configures a local pool of static addresses to be used in assigning IP addresses to mobile nodes in the cisco.com domain:

```
ip mobile host nai @cisco.com static-address local-pool mobilenodes
```

The following example configures a local pool of dynamic addresses to be used in assigning IP addresses to mobile nodes in the cisco.com domain. The security associations that are retrieved from the AAA server are cached permanently until cleared manually.

```
ip mobile host nai @cisco.com address pool local mobilenodes virtual network 10.2.0.0
255.255.0.0 aaa load-sa permanent lifetime 180
```

The following example configures the DHCP proxy client to use a DHCP server located at 10.1.2.3 to allocate a dynamic home address:

```
ip mobile host nai @dhcppool.com address pool dhcp-proxy-client dhcp-server 10.1.2.3 interface
 FastEthernet 0/0
```

Related Commands

Command	Description
aaa authorization ipmobile	Authorizes Mobile IP to retrieve security associations from the AAA server using TACACS+ or RADIUS.
clear ip mobile secure	Clears and retrieves remote security associations.
ip mobile proxy-host	Locally configures the proxy Mobile IP attributes
ip mobile secure	Specifies the mobility security associations for mobile host, visitor, home agent, and foreign agent.
show ip mobile host	Displays mobile node counters and information.

logical-mn

To enable mobile router functionality in MAG, use the **logical-mn** command in MAG configuration mode. To disable the mobile router functionality, use the **no** form of this command.

logical-mn *network-access-identifier*

no logical-mn *network-access-identifier*

Syntax Description

network-access-identifier	Specifies the Network Access Identifier (NAI) of the mobile node.

Command Default

The mobile router functionality is not enabled.

Command Modes

MAG configuration (config-ipv6-pmipv6-mag)

Command History

Release	Modification
15.4(1)T	This command was introduced.

Usage Guidelines

Only loopback interfaces can be configured as home interfaces. A loopback interface that is configured as home interface must first be configured as a MAG-enabled interface.

Examples

The following example shows how to enable the mobile router:

```
Device(config)# ipv6 mobile pmipv6-mag mag1 domain dn1
Device(config-ipv6-pmipv6-mag)# logical-mn mn1@example.com
Device(config-ipv6-pmipv6-mag-logicalmn)#
```

Related Commands

Command	Description
nai	Configures the NAI for the MN within the PMIPV6 domain.

mcsa

To enable mobile client service abstraction (MCSA), use the **mcsa** command in global configuration mode. To disable MCSA, use the **no** form of this command.

mcsa

no mcsa

Syntax Description

There are no arguments and keywords.

Command Default

An abstraction to receive event notifications is not available.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.8S	This command was introduced in Cisco IOS XE Release 3.8S.

Usage Guidelines

MCSA provides an abstraction to receive the discovery event and service event notifications from the MNs, and binding events from the local mobility anchor (LMA).

If you have enabled the mobile access gateway (MAG) functionality, you do not have to enable the **mcsa** command.

Enter the **sessionmgr** command in MAG configuration mode, before you enter the **mcsa** command in global configuration mode.

Enter the **no sessionmgr** command in MAG configuration mode, before you enter the **no mcsa** command in global configuration mode.

Examples

The following example shows how to enable MCSA:

```
Device# configuration terminal
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) sessionmgr
Device(config-ipv6-pmipv6-mag) exit
Device(config) mcsa
```

The following example shows how to disable MCSA:

```
Device# configuration terminal
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) no sessionmgr
Device(config-ipv6-pmipv6-mag) exit
Device(config) no mcsa
```

Related Commands

Command	Description
show mcsa statistics	Displays the MCSA notification statistics.

mobile network (label)

To configure a physical interface for a mobile network, use the **mobile network** command in MAG logical MN configuration. To disassociate a physical interface from the mobile network, use the **no** form of this command.

mobile network *interface-name interface-type* **label** *label-name* [*skip-register*]

no mobile network *interface-type interface-number*

Syntax Description

interface-ype	Interface type.
interface-number	Interface number.
label *label-name*	A identifier for the interface to be used in the PMIPv6 signaling packets.
skip-register	(Optional) Specified when the interface information is not to be carried in the PMIPv6 proxy binding update (PBU) packet.

Command Default

No mobile networks are configured.

Command Modes

MAG logical MN configuration (config-ipv6-pmipv6-mag-logicalmn)

Command History

Release	Modification
15.4(1)T	This command was introduced.

Usage Guidelines

Do not use a MAG-enabled interface for the mobile network.

Examples

```
Device(config)# ipv6 mobile pmipv6-mag mag1 domain dn1
Device(config-ipv6-pmipv6-mag)# logical-mn mn1@example.com
Device(config-ipv6-pmipv6-mag-logicalmn)# mobile network ethernet 0/0 label eth0
```

Related Commands

Command	Description
interface	Configures an interface on which the MAG is enabled.

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 fffffff
```

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
```

nai (proxy mobile ipv6) through tunnel mode gre

network

To associate a network, to which an IPv4 or IPv6 pool can be configured, with a Local Mobility Anchor (LMA) or a mobile node (MN), use the **network** command in LMA configuration mode or MN configuration mode. To disassociate the network from the LMA or MN, use the **no** form of this command.

network *name*

no network *name*

Syntax Description

name	Name of the network to be associate with the LMA.

Command Default

No network is associated.

Command Modes

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

LMA configuration mode (config-ipv6-pmipv6-lma)

Command History

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

Usage Guidelines

Use the **network** command in LMA configuration mode or MN configuration mode, to associate a network, to which an IPv4 or IPv6 pool can be configured, with an LMA or MN. You can associate only one IPv4 or IPv6 pool to a network. The name of the network configured in an LMA is recorded as an attribute in the MN profile.

Examples

The following example shows how to associate a network with an LMA:

```
Device(config)# ipv6 mobile pmipv6-lma lma1 domain dn1
Device(config-ipv6-pmipv6-lma)# address ipv4 192.0.2.1
Device(config-ipv6-pmipv6-lma)# network network1
```

The following example shows how to associate a network to with an MN:

```
Device(config)# ipv6 mobile pmipv6-domain dn1
Device(config-ipv6-pmipv6-domain)# nai example1@example.com
Device(config-ipv6-pmipv6-domain-mn)# network network1
```

Related Commands

Command	Description
ipv6 mobile pmipv6-lma	Configures the LMA for the PMIP domain.

Command	Description
ipv6 mobile pmipv6-domain	Configures a PMIP domain.

nai (proxy mobile IPv6)

To configure the Network Access Identifier (NAI) for the mobile node (MN) within the PMIPV6 domain, use the **nai** command in PMIPV6 domain configuration mode. To disable the NAI configuration, use the **no** form of this command.

nai [*user*] *@realm*

no nai [*user*] *@realm*

Syntax Description

user@realm	Fully qualified specific user address and realm. The @ symbol is required.
@realm	Any user address at a specific realm. The @ symbol is required.

Command Default

NAI for the MN is not specified.

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.

Examples

The following example shows how to configure the NAI within the PMIPV6 domain:

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

Related Commands

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

network (mobile networks)

To specify a list of mobile networks for a mobile router, use the **network** command in mobile networks configuration mode. To remove an entry, use the **no** form of this command.

network *net mask*

no network *net mask*

Syntax Description

net	IP address of the directly connected networks.
mask	Network mask.

Command Default

No networks are specified.

Command Modes

Mobile networks configuration

Command History

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

Usage Guidelines

When the mobile router is registered, the home agent injects the mobile networks into its routing table.

Examples

The following configuration example shows how to associate the mobile router address, 10.1.1.10, with the mobile networks:

Examples

```
ip mobile router
  address 10.1.1.10 255.255.255.0
  home-agent 10.1.1.20
ip mobile secure home-agent 10.1.1.20 spi 100 key hex 12345678123456781234567812345678
```

Examples

```
! mobile host is mobile router address
ip mobile host 10.1.1.10 virtual-network 10.0.0.0 255.0.0.0
! associates mobile router address with mobile networks
ip mobile mobile-networks 10.1.1.10
  description jet
  network 172.6.1.0 255.255.255.0
ip mobile secure host 10.1.1.10 spi 100 key hex 12345678123456781234567812345678
```

Related Commands

Command	Description
show ip mobile mobile-networks	Displays a list of mobile networks associated with the mobile router.

outdscp

To specify a differentiated services code point (DSCP) value used for the outbound IP multiplexed superframe for the policy, use the **outdscp** 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.

outdscp *DSCP-value*

no outdscp

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

Superframes are sent with the DSCP bit set to 0.

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

If you do not enter a value for the **outdscp** command, superframes are sent with the DSCP bit set as 0.

Examples

The following example shows how to configure the DSCP value to 10 for the outbound multiplexed superframe in the IPv6 multiplexing policy *routeRTP-SJ* :

```
Router# configure terminal
Router(config)# ipv6 mux policy routeRTP-SJ
Router(config-ipmux-policy-v6)# outdscp 10
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.

physical-interface

To create a physical subinterface and to associate it with the Virtual Multipoint Interface (VMI) on a router, use the **physical-interface** command in interface configuration mode. To return to the default mode, use the **no** form of this command.

physical-interface *interface-type*/*slot*

no physical-interface *interface-type*/*slot*

Syntax Description

interface-type	Type of interface or subinterface.
/ *slot*	Slot in which the interface is present.

Command Default

No physical interface exists.

Command Modes

Interface configuration (config-if)

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 VMIs in Mobile Adhoc Router-to-Radio Networks.
12.4(24)T	This command was modified. This command supports the subinterfaces and VLANS associated with an interface.

Usage Guidelines

The **physical-interface** command supports the subinterfaces and VLANs associated with an interface. This command also allows VMI interface to operate over encapsulated interfaces, if required. Only one physical interface can be assigned to a VMI interface. Because there is very high number of VMI interfaces that can be used, assign a new VMI for each physical interface.

Examples

The following example shows how to create a physical subinterface:

```
Router(config)# interface vmi1
Router(config-if)# physical-interface FastEthernet0/1
```

Related Commands

Command	Description
debug vmi	Displays debugging output for VMIs.
eigrp interface	Sets a threshold value to minimize hysteresis in a router-to-radio configuration.
interface vmi	Creates a VMI interface.
mode bypass	Enables VMIs to support multicast traffic

pool ipv4

To specify the name of the IPv4 address pool, from which a home address is allocated to a mobile node (MN), in a Local Mobility Anchor (LMA), use the **pool ipv4** command in LMA-network configuration mode. To disassociate an IPv4 address pool from an LMA, use the **no** form of this command.

pool ipv4*name* **pfxlen** *length*

no pool ipv4*name* **pfxlen** *length*

Syntax Description

name	Name of the IPv4 address pool.
pfxlen *length*	Specifies the prefix length of the pool address.

Command Default

No IPv4 address pool is specified in the LMA for the MN.

Command Modes

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

Command History

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

Usage Guidelines

Configure the **ip local pool** command in global configuration mode before using the **pool ipv4** command. Use the same pool name that you specified in the **ip local pool** command, in the **pool ipv4** command.

Use the **pool ipv4** command in LMA-network configuration mode to specify the name of the IPv4 address pool, from which a home address is allocated to a MN subscriber, in a Local Mobility Anchor (LMA).

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)# pool ipv4 v4pool pfxlen 24
```

Related Commands

Command	Description
ip local pool	Configures a local pool of IPv4 addresses.

pool ipv6

To specify the name of the IPv6 prefix pool, from which a home network prefix is allocated to a mobile node (MN), in a Local Mobility Anchor (LMA), use the **pool ipv6** command in LMA-network configuration mode. To disassociate an IPv6 prefix pool from an LMA, use the **no** form of this command.

pool ipv6*name* **pfxlen** *length*

no pool ipv6*name* **pfxlen** *length*

Syntax Description

name	Name of the IPv6 prefix pool.
pfxlen *length*	Specifies the prefix length of the pool address.

Command Default

No IPv6 address pool is specified in the LMA for the MN.

Command Modes

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

Command History

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

Usage Guidelines

Configure the **ipv6 local pool** in global configuration mode before using the **pool ipv6** command. Use the same pool name that you specified in the **ipv6 local pool** command, in the **pool ipv6** command.

Use the **pool ipv6** command in LMA-network configuration mode to specify the name of the IPv4 address pool, from which a home address is allocated to a mobile node (MN) subscriber, in a Local Mobility Anchor (LMA).

Examples

The following example shows how to specify the name of the IPv6 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)# pool ipv4 v4pool pfxlen 24
```

Related Commands

Command	Description
ipv6 local pool	Configures a local pool of IPv6 prefixes.

rat

To set the priority of a Radio Access Technology (RAT) type, use the **rat** command in the third-generation mobility anchor (3GMA) role configuration mode. To remove the priority of a RAT type, use the **no** form of this command.

rat *rat-type* **priority** *priority-number*

no rat *rat-type* **priority** *priority-number*

Syntax Description

rat-type	Specifies the RAT type.
priority *priority-number*	Specifies the priority number for the RAT type.

Command Default

None

Command Modes

3GMA role configuration (config-ipv6-pmipv6lma-role)

Command History

Release	Modification
Cisco IOS XE Release 3.9S	This command was introduced.

Usage Guidelines

The mobility anchor routes packets through tunnels associated with RAT of higher priority. You can set the same priority number for multiple RAT types for load balancing for downstream traffic. For example, you can set priority number 2 to Worldwide Interoperability for Microwave Access(WIMAX) and Wireless Local Area Network (WLAN). The mobility anchor balances traffic and forwards packets by sharing packets between WIMAX and WLAN tunnels.

Examples

The following example show how to set 2 as the priority for WIMAX:

```
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)# rat wimax priority 2
```

The following example show how to set 2 as the priority for WLAN:

```
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)# rat wlan priority 2
```

Related Commands

Command	Description
ipv6 mobile pmipv6-lma	Configures the LMA for the PMIP domain.
ipv6 mobile pmipv6-domain	Configures a PMIPv6 domain.

redundancy group

To configure fault tolerance for the mobile router, use the **redundancy group** command in mobile router configuration mode. To disable this functionality, use the **no** form of this command.

redundancy group *name*

no redundancy group *name*

Syntax Description

name	Name of the mobile router group.

Command Default

No default behavior or values.

Command Modes

Mobile router configuration

Command History

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

Usage Guidelines

The **redundancy group** command provides f ault tolerance by selecting one mobile router in the redundancy group *name* argument to provide connectivity for the mobile networks. This mobile router is in the active state. The other mobile routers are passive and wait until the active mobile router fails before a new active mobile router is selected. Only the active mobile router registers and sets up proper routing for the mobile networks. The redundancy state is either active or passive.

Examples

The following example selects the mobile router in the sanjose group, to provide fault tolerance:

```
ip mobile router
 redundancy group sanjose
 address 10.1.1.10 255.255.255.0
 home-agent 10.1.1.20
 register lifetime 600
```

Related Commands

Command	Description
standby name	Configures the name of the standby group, which is associated with the mobile router.

register (mobile networks)

To dynamically register the mobile networks with the home agent, use the **register** command in mobile networks configuration mode. To disable the registration, use the **no** form of this command.

register

no register

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

Mobile networks configuration

Command History

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

Usage Guidelines

When the mobile router registers its mobile networks on the home agent, the home agent looks up the mobile network configuration and verifies that the **register** command is configured before adding forwarding entries into the home agent forwarding table for the mobile router. If the mobile router is not configured properly, the home agent will reject the request with error code 129.

It is possible to have both statically configured mobile networks and dynamically registered mobile networks. However, static mobile network configurations take precedence over dynamic mobile network registrations. For example, if a mobile router tries to dynamically add (or delete) a mobile network and that network is already statically configured for that mobile router or any other mobile router, then the dynamic mobile network is ignored and an error message is generated.

Similarly, if a mobile router has dynamically added a mobile network, an attempt by another mobile router to dynamically add or delete the same mobile network is ignored and an error message is generated.

Examples

In the following example, the mobile router is configured to dynamically register its mobile networks with the home agent:

```
router mobile
 ip mobile home-agent
 ip mobile host 10.20.30.4 interface Ethernet 1
!Associated host address that informs HA that 10.20.30.4 is actually an MR
 ip mobile mobile-networks 10.20.30.4
  register
ip mobile secure host 10.20.30.4 spi 100 key hex 12345678123456781234567812345678
```

Related Commands

Command	Description
ip mobile host	Configures the mobile host or mobile node group.
mobile-network	Specifies the mobile router interface that is connected to the dynamic mobile network.

register (mobile router)

To con trol the registration parameters of the IPv6 mobile router, use the **register** command in mobile router configuration mode or IPv6 mobile router configuration mode. To return the registration parameters to their default settings, use the **no** form of this command.

register {**extend expire** *seconds* **retry** *number* **interval** *seconds*| **lifetime** *seconds*| **retransmit initial milliseconds maximum milliseconds retry number**}

no register {**extend expire** *seconds* **retry** *number* **interval** *seconds*| **lifetime** *seconds*| **retransmit initial milliseconds maximum milliseconds retry number**}

Syntax Description

extend	Reregisters before the lifetime expires.
expire *seconds*	Specifies the time (in seconds) in which to send a registration request before expiration. In IPv4, the range is from 1 to 3600; the default is 120. In IPv6, the range is from 1 to 600.
retry *number*	Specifies the number of times the mobile router retries sending a registration request if no reply is received. In both IPv4 and IPv6, the range is from 0 to 10; the default is 3. A value of 0 means no retry. The mobile router stops sending registration requests after the maximum number of retries is attempted.
interval *seconds*	Specifies the time (in seconds) that the mobile router waits before sending another registration request if no reply is received. In IPv4, the range is from 1 to 3600; the default is 10. In IPv6, the range is from 1 to 60.
lifetime *seconds*	Specifies the requested lifetime (in seconds) of each registration. The shortest value between the configured lifetime and the foreign agent advertised registration lifetime is used. In IPv4, the range is from 3 to 65534; the default is 65534 (infinity). In IPv6, the range is from 4 to 262143; the default is 262143 (infinity). This default ensures that the advertised lifetime is used, excluding infinity.
retransmit initial *milliseconds*	Specifies the wait period (in milliseconds) before sending a retransmission the first time no reply is received from the foreign agent. In IPv4, the range is from 10 to 10000 milliseconds (10 seconds); the default is 1000 milliseconds (1 second). In IPv6, the range is from 1000 to 256000.

maximum *milliseconds* **retry** *number*	Specifies the maximum wait period (in milliseconds) before retransmission of a registration request. In IPv4, the range is 10 to 10000 (10 seconds); the default is 5000 milliseconds (5 seconds). In IPv6, the maximum range is from 1000 to 256000. In IPv6, the retry number range is from 0 to 10. Each successive retransmission timeout period is twice the previous period, if the previous period was less than the maximum value. Retransmission stops after the maximum number of retries.

Command Default

The registration parameters of the IPv6 mobile router are used.

Command Modes

Mobile router configuration IPv6 mobile router configuration (IPv6-mobile-router)

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.4(20)T	Support for IPv6 was added.

Usage Guidelines

The **register lifetime***seconds*command configures the lifetime that the mobile router requests in a registration request. The home agent also has lifetimes that are set. If the registration request from a mobile router has a greater lifetime than the registration reply from the home agent, the lifetime set on the home agent will be used for the registration. If the registration request lifetime from the mobile router is less than the registration reply from the home agent, the lifetime set on the mobile router will be used. Thus, the smaller lifetime between the home agent and mobile router is used for registration.

Examples

The following example specifies a registration lifetime of 600 seconds:

```
ip mobile router
 address 10.1.1.10 255.255.255.0
 home-agent 10.1.1.20
 register lifetime 600
```

Related Commands

Command	Description
ipv6 mobile router	Enables IPv6 NEMO functionality on the router and places the router in IPv6 mobile router mode.
show ip mobile router	Displays configuration information and monitoring statistics about the mobile router.

Command	Description
show ip mobile router registration	Displays the pending and accepted registrations of the mobile router.

replay-protection

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

replay-protection timestamp [**window** *seconds*]

no replay-protection timestamp

Syntax Description

timestamp	Enables the time stamp.
window *seconds*	(Optional) Specifies the maximum time difference, in seconds, between the time stamp in the received Proxy Binding Update (PBU) message and the current time of day on the Local Mobility Anchor (LMA). • The range is from 1 to 255.

Command Default

The replay protection mechanism is configured with the default time stamp window period is 7 seconds.

Command Modes

LMA configuration (config-ipv6-pmipv6-lma)

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

Usage Guidelines

The window period is the maximum time difference, in seconds, between the time stamp in the received PBU message and the current time of day on the LMA that is allowed by the LMA for the received message to be considered valid. The **timestamp window** *seconds* keyword-argument pair is the TimestampValidityWindow configuration variable that is documented in RFC 5213, where the default value for the variable is 300 milliseconds, which must be adjusted to suit the deployment.

Use the **replay-protection** command in PMIPV6 domain configuration mode to configure the replay protection mechanism within the Proxy Mobile IPv6 (PMIPv6) domain.

Use the **replay-protection** command in MAG configuration mode to configure the replay protection mechanism within the MAG.

Use the **replay-protection** command in LMA configuration mode to configure the replay protection mechanism within the LMA.

Use the **replay-protection timestamp** command in PMIPV6 domain configuration mode to configure the replay protection mechanism. If the PMIPV6 domain is configured using the **ipv6 mobile pmipv6-domain** *domain-name* **load-aaa** command, use the **replay-protection timestamp** command to override the time stamp configuration.

Use the **replay-protection timestamp** command in MAG configuration mode to configure the replay protection mechanism for the MAG.

While configuring the **replay-protection timestamp** command, preferably configure Network Time Protocol (NTP) in the device. If the device clocks are not configured with NTP, synchronize the clocks manually.

Examples

The following example shows how to configure the replay protection mechanism with a window period of 200 seconds within the PMIPV6 domain:

```
Device(config)# ipv6 mobile pmipv6-domain dn1
Device(config-ipv6-pmipv6-domain)# replay-protection timestamp window 200
```

The following example shows how to reset the replay protection mechanism to the default window period 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)# no replay-protection timestamp
```

The following example shows how to reset the replay protection mechanism to the default window period 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-mag)# no replay-protection timestamp
```

Related Commands

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

reverse-tunnel

To enable the reverse tunnel function on the mobile router, use the **reverse-tunnel**command in mobile router configuration mode. To disable the reverse tunnel function, use the **no** form of this command.

reverse-tunnel

no reverse-tunnel

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

Mobile router configuration

Command History

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

Examples

The following example configures reverse tunneling on the mobile router:

```
ip mobile router
 address 10.1.1.2 255.0.0.0
 home-agent 10.1.1.1
 register extend expire 10 retry 2 interval 2
 reverse-tunnel
```

Related Commands

Command	Description
show ip mobile router	Displays configuration information and monitoring statistics about the mobile router.
show ip mobile router registration	Displays the pending and accepted registrations of the mobile router.
show ip mobile tunnel	Displays active tunnels.

roaming interface

To specify an interface as a roaming interface for a Mobile Access Gateway (MAG) and set its parameters, use the **roaming interface** command in the MAG dynamic address configuration mode. To stop an interface from being a roaming interface, use the **no** form of this command.

roaming interface *type number* **priority** *priority-value* **egress-att** *access-tech-type* **label** *egress-label*

no roaming interface *type number*

Syntax Description

interface *typenumber*	Specifies an interface as the roaming interface.
priority *priority-value*	Specifies the priority value for the roaming interface. The range is from 1 to 100.
egress-att *access-tech-type*	Specifies the access technology type of the roaming interface.
label *egress-label*	Specifies the label for the roaming interface. It can be one of the following values: • Ethernet • WLAN (Wireless LAN) • 3G (third generation) • LTE (Long Term Evolution)

Command Default

No roaming interfaces are specified for the MAG.

Command Modes

MAG dynamic address configuration (config-ipv6-pmipv6-mag-addr-dyn)

Command History

Release	Modification
15.4(1)T	This command was introduced.

Usage Guidelines

When the multipath feature is not involved in the roaming interface, the higher the priority value that is set in the interface the greater is the preference given to the interface specified as the roaming interface. However, when the multipath feature is involved, the priority value does not make a difference.

Examples

The following example shows how to specify an interface as the roaming interface for the MAG:

```
Device(config)# ipv6 mobile pmipv6-mag mag1 domain dn1
Device(config-ipv6-pmipv6-mag)# address dynamic
Device(config-ipv6-pmipv6-mag-addr-dyn)# roaming interface ethernet 0/0 priority 2 egress-att
 LTE label egress1
```

Related Commands

Command	Description
multipath	Enables multipath support in LMA.

role

To configure the role of the Mobile Access Gateway (MAG), use the **role** command in MAG configuration mode. To remove the configuration, use the **no** form of this command.

role {**3gpp| lte| wimax| wlan**}

no role {**3gpp| lte| wimax| wlan**}

Syntax Description

3gpp	Specifies the role as third Generation Partnership Project (3GPP).
lte	Specifies the role as Long Term Evaluation (LTE).
wimax	Specifies the role as WiMAX.
wlan	Specifies the role as wireless LAN (WLAN).

Command Default

The default role is WLAN.

Command Modes

MAG configuration (config-ipv6-pmipv6-mag)

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

The default role, WLAN, cannot be disabled, but can only be configured to 3GPP, LTE, or WiMAX.

In Cisco IOS XE Release 3.4S and Cisco IOS Release 15.2(4)M, the only supported roles for the MAG are 3GPP and WLAN.

Examples

The following example shows how to configure the role of the MAG as 3GPP:

```
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)# role 3gpp
```

Related Commands

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

role 3gma

To enable the third-generation mobility anchor (3GMA) functionality, use the **role 3gma** command in Local Mobility Anchor (LMA) configuration mode. To disable 3GMA functionality, use the **no** form of this command.

role 3gma

no role 3gma

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

LMA configuration (config-ipv6-pmipv6-lma)

Command History

Release	Modification
Cisco IOS XE Release 3.9S	This command was introduced.

Usage Guidelines

The **role 3gma** command can be used only in the LMA configuration mode.

Examples

The following example shows how to configure the 3GMA functionality:

```
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)# role 3gma
```

Related Commands

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

router mobile

To enable Mobile IP on the router, use the **router mobile** command in global configuration mode. To disable Mobile IP, use the **no** form of this command.

router mobile

no router mobile

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration

Command History

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

Usage Guidelines

This command must be used in order to run Mobile IP on the router, as either a home agent or a foreign agent. The process is started, and counters begin. Disabling Mobile IP removes all related configuration commands, both global and interface.

Examples

The following example enables Mobile IP:

```
router mobile
```

Related Commands

Command	Description
show ip mobile globals	Displays global information for mobile agents.
show ip protocols	Displays the parameters and current state of the active routing protocol process.
show processes	Displays information about the active processes.

sessionmgr

To enable mobile access gateway (MAG) to process the notifications it receives through the mobile client service abstraction (MCSA) from Intelligent Services Gateway (ISG), use the **sessionmgr** command in MAG configuration mode. To disable this function, use the **no** form of this command.

sessionmgr

no sessionmgr

Syntax Description

This command does not have any arguments or keywords.

Command Default

MAG does not process the notification it receives through MCSA from the ISG.

Command Modes

MAG configuration (config-ipv6-pmipv6-mag)

Command History

Release	Modification
Cisco IOS XE Release 3.8S	This command was introduced.

Usage Guidelines

This command is not supported in standalone MAG configuration. Use this command only when a MAG is configured to coexist with an ISG.

Examples

The following example shows how to enable the MAG to process the notifications it receives through MCSA from the ISG:

```
Device> enable
Device# configuration terminal
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)# sessionmgr
```

service (proxy mobile IPv6)

To configure the service provided to a mobile node (MN), use the **service** command in PMIPV6 domain mobile node configuration mode. To disable the service configuration, use the **no** form of this command.

Cisco IOS XE Release 3.4S

service ipv4

no service ipv4

Cisco IOS XE Release 3.7S and Later Releases

service {**dual**| **ipv4**| **ipv6**}

no service{**dual**| **ipv4**| **ipv6**}

Syntax Description

dual	Configures both IPv4 and IPv6 services to an MN.
ipv4	Configures the IPv4 service to an MN. This is the default.
ipv6	Configures the IPv6 service to an MN.

Command Default

The IPv4 service is provided to 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.
Cisco IOS XE Release 3.5S	This command was modified. The **dual** and **ipv6** keywords were added.
15.2(4)M	This command was integrated into Cisco IOS Release 15.2(4)M.

Examples

The following example shows how to provide the IPv6 service to the MN:

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

Related Commands

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

set link-type

To specify the link type for a match clause, use the **set link-type** command in PMIPv6 domain mobile-map configuration mode. To disable this function, use the **no** form of this command.

set link-type *link-name1* [*link-name2*] [*link-name3*] [*null*]

no set link-type

Syntax Description

link-name1	Name of the outgoing interface link type.
link-name2	Name of the outgoing interface link type.
link-name3	Name of the outgoing interface link type.
null	Drops the traffic that matches the configured access-list.

Command Default

No link type exists for the configured match clause.

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

Create a match clause in the mobile-map configuration mode. Use the **set link-type** command to choose the appropriate outgoing interface types that match the configured access-list.

Examples

The following example shows how to specify the link types for a match clause:

```
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
Device(config-ipv6-pmipv6-domain-mobile-map)# set link-type wifi 3g lte null
```

Related Commands

Command	Description
match access-list	Creates a match clause and specifies access lists.

show ip mobile aaa requests host

To display pending requests sent to the accounting, authentication, and authorization (AAA) host, use the **show ip mobile aaa requests host**command in privileged EXEC mode.

show ip mobile aaa requests host [*ip-address*| **nai** *network-address-id*]

Syntax Description

ip-address	(Optional) IP address of the mobile node (MN).
nai *network -address-id*	(Optional) Specifies the network access identifier (NAI) of the mobile node.

Command Modes

Privileged EXEC (#)

Command Default

If the IP address of a mobile node is not specified, information for all mobile nodes is displayed.

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.

Examples

The following is sample output from the **show ip mobile aaa requests host** command for IP address 192.168.0.0:

```
Router# show ip mobile aaa requests host 192.168.0.0
Host 1.1.1.1 has sent author request to AAA
Reason: HOST_AUTHEN
```

The following is sample output from the **show ip mobile aaa requests host** command for network access identifier user06@example.com:

```
Router# show ip mobile aaa requests host
 nai user06@example.com
Host user06@cisco.com has sent author request to AAA
Reason: HOST_AUTHEN
```

Related Commands

Command	Description
show ip mobile host	Displays mobile node information.

show ip mobile binding

To display the mobility binding table on the home agent (HA), use the **show ip mobile binding**command in privileged EXEC mode.

show ip mobile binding [**home-agent** *ip-address*| **nai** *string* [**session-id** *string*]| **summary**]

Syntax Description

home-agent	(Optional) Mobility bindings for a specific home agent (HA).
ip-address	(Optional) IP address for the HA.
nai *string*	(Optional) Mobile node (MN) identified by the network access identifier (NAI).
session-id *string*	(Optional) Session identifier. The *string* argument must be fewer than 25 characters in length.
summary	(Optional) Total number of bindings in the table.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.0(2)T	The **home-agent**keyword and *ip-address*argument were added.
12.1(2)T	The **summary** keyword was added.
12.2(2)XC	The nai keyword was added.
12.2(13)T	This command was enhanced to display the service options field and to include information about the mobile networks registered on the home agent.
12.3(4)T	The **session-id** keyword was added.
12.3(8)T	The output was enhanced to display UDP tunneling information.
12.4(9)T	The output was enhanced to display multipath support.

Usage Guidelines

You can display a list of all bindings if you press enter. You can also specify an IP address for a specific home agent using the **show ip mobile binding home-agent** *ip-address*command.

If the **session-id** *string* combination is specified, only the binding entry for that session identifier is displayed. A session identifier is used to uniquely identify a Mobile IP flow. A Mobile IP flow is the set of {NAI, IP address}. The flow allows a single NAI to be associated with one or multiple IP addresses, for example, {NAI, ipaddr1}, {NAI, ipaddr2}, and so on. A single user can have multiple sessions for example, when logging through different devices such as a PDA, cellular phone, or laptop. If the session identifier is present in the initial registration, it must be present in all subsequent registration renewals from that MN.

Examples

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

```
Router# show ip mobile binding
Mobility Binding List:
Total 1
10.0.0.1:
 Care-of Addr 10.0.0.31, Src Addr 10.0.0.31,
 Lifetime granted 02:46:40 (10000), remaining 02:46:32
 Flags SbdmGvt, Identification B750FAC4.C28F56A8,
 Tunnel100 src 10.0.0.5 dest 10.0.0.31 reverse-allowed
 Routing Options - (G)GRE
  Service Options:
  NAT detect
```

The following is sample output from the **show ip mobile binding**command when mobile networks are configured or registered on the home agent:

```
Router# show ip mobile binding
Mobility Binding List:
Total 1
10.0.4.1:
 Care-of Addr 10.0.0.5, Src Addr 10.0.0.5
 Lifetime granted 00:02:00 (120), remaining 00:01:56
 Flags sbDmgvT, Identification B7A262C5.DE43E6F4
 Tunnel0 src 10.0.0.3 dest 10.0.0.5 reverse-allowed
 MR Tunnel1 src 10.0.0.3 dest 10.0.4.1 reverse-allowed
 Routing Options - (D)Direct-to-MN (T)Reverse-tunnel
 Mobile Networks: 10.0.0.0/255.255.255.0(S)
  10.0.0.0/255.255.255.0 (D)
  10.0.0.0/255.0.0.0(D)
```

The following is sample output from the **show ip mobile binding**command with session identifier information:

```
Router# show ip mobile binding
Mobility Binding List:
Total 1
 10.100.100.19:
 Care-of Addr 10.70.70.2, Src Addr 10.100.100.1,
 Lifetime granted 00:33:20 (20000), remaining 00:30:56
 Flags SbdmGvt, Identification BC1C2A04.EA42659C,
 Tunnel0 src 10.100.100.100 dest 10.70.70.2 reverse-allowed
 Routing Options
 Session identifier 998811234
 SPI 333 (decimal 819) MD5, Prefix-suffix, Timestamp +/-255, root key
 Key 38a38987ad0a399cb80940835689da66
 SPI 334 (decimal 820) MD5, Prefix-suffix, Timestamp +/-255, session key
 Key 34c7635a313038611dec8c16681b55e0
```

The following sample output shows that the home agent is configured to detect network address translation (NAT):

```
Router# show ip mobile binding nai mn@cisco.com
Mobility Binding List:
 mn@cisco.com (Bindings 1):
 Home Addr 10.99.101.1
 Care-of Addr 192.168.1.202, Src Addr 192.168.157.1
 Lifetime granted 00:03:00 (180), remaining 00:02:20
 Flags sbDmg-T-, Identification BCF5F7FF.92C1006F
 Tunnel0 src 192.168.202.1 dest 192.168.157.1 reverse-allowed
 Routing Options - (D)Direct-to-MN (T)Reverse-tunnel
 Service Options:
 NAT detect
```

The following sample output shows that multipath support is enabled:

```
Router# show ip mobile binding
Mobility Binding List:
Total 1
10.1.1.1:
    Care-of Addr 10.1.1.11, Src Addr 10.1.1.11
    Lifetime granted 10:00:00 (36000), remaining 09:52:40
    Flags sbDmg-T-, Identification C5441314.61D36B14
    Tunnel1 src 12.1.1.10 dest 10.1.1.11 reverse-allowed
    MR Tunnel1 src 12.1.1.10 dest 10.1.1.11 reverse-allowed
    Routing Options - (D)Direct-to-MN (T)Reverse-tunnel
    Mobile Networks: 10.38.0.0/255.255.0.0 (D)
    Roaming IF Attributes: BW 10000 Kbit, ID 3247
     Description First Lan Interface
    Multi-path Metric bandwidth
```

The below table describes the significant fields shown in the display.

Table 9: show ip mobile binding Field Descriptions

Field	Description
Total	Total number of mobility bindings.
<IP Address>	Home IP address of the mobile node. The NAI is displayed if configured.
Care-of Addr	Care-of address of the mobile node.
Src Addr	IP source address of the registration request as received by the home agent. Will be either the colocated care-of address of a mobile node or an address on the foreign agent or the active HA address. If it is the active HA address, then this is a binding update from the active HA to the standby HA and not a registration directly received from the MN or FA.
Lifetime granted	The lifetime (in hh:mm:ss) granted to the mobile node for this registration. Number of seconds appears in parentheses.
remaining	The time (in hh:mm:ss) remaining until the registration expires. It has the same initial value as lifetime granted and is counted down by the home agent.

Field	Description
Flags	Services requested by the mobile node. The mobile node requests these services by setting bits in the registration request. Uppercase characters denote bit set.
Identification	Identification used in that binding by the mobile node. This field has two purposes: unique identifier for each request and replay protection.
Tunnel	The tunnel used by the mobile node is characterized by the source and destination addresses and reverse-allowed or reverse-off for reverse tunnel. The default encapsulation is IP-in-IP. The mobile node can request GRE.
Routing Options	Routing options identify the services that the home agent is currently providing. The mobile node must request these services in its registration request by setting the services flag (see Flags field description). For example, the V bit may have been requested by the mobile node (shown in the Flags field), but the home agent will not provide such service. Possible options are B (broadcast), D (direct-to-mobile node), G (GRE), and T (reverse-tunnel).
Service Options	Service options configured.
NAT detect	Indicates that the mobile node is registering from behind a NAT-enabled router.
Mobile Networks	Mobile networks configured or registered on the home agent. D denotes dynamic (registered) mobile networks, and S denotes static (configured) mobile networks.
Session identifier	The ID used to uniquely identify a Mobile IP flow.
SPI	The security parameter index (SPI) is the 4-byte opaque index within the mobility security association that selects the specific security parameters to be used to authenticate the peer.
MD5	Message Digest 5 authentication algorithm. HMAC-MD5 is displayed if configured.
Prefix-suffix	Authentication mode.
Timestamp	Replay protection method.

Field	Description
root key	Dynamic key based on the Microsoft Windows password shared between the mobile node and AAA or Windows domain controller or active directory. Once a mobile node registers, this key is established until the binding persists on the home agent. Subsequent registration requests can be authenticated using the root key.
session key	Dynamic key that is derived using the root key. This key can be refreshed, and the refreshed keys are based off the root key. Subsequent registration renewal messages can be authenticated using the session key. The period or frequency for the session key refresh is determined by the mobile node. Registration requests that also request session key refresh are authenticated using the root key.
Roaming IF Attributes	Attributes associated with the roaming interface. BW denotes the bandwidth of the roaming interface.
Description	Description of the roaming interface on the mobile router.
Multi-path Metric bandwidth	Metric that the mobile router uses for multipath support.

Related Commands

Command	Description
debug ip mobile	Displays IP mobility activities.
ip mobile foreign-agent nat traversal	Enables NAT UDP traversal support for Mobile IP foreign agents.
ip mobile home-agent nat traversal	Enables NAT UDP traversal support for Mobile IP HAs.
show ip mobile globals	Displays global information about Mobile IP home agents, foreign agents, and mobile nodes.
show ip mobile tunnel	Displays information about UDP tunneling.
show ip mobile visitor	Displays the table that contains a visitor list of foreign agents.

show ip mobile globals

To display global information for mobile agents, use the **show ip mobile globals**command in privileged EXEC mode.

show ip mobile globals

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2(13)T	This command was enhanced to display the NAT detect field and the Strip realm domain field.
12.2(15)T	This command was enhanced to display the HA Accounting field.
12.3(7)T	This command was enhanced to display information about foreign agent route optimization.
12.3(8)T	This command was enhanced to display information about UDP tunneling.
12.4(9)T	This command was enhanced to display information about multipath support.

Usage Guidelines

This command shows the services provided by the home agent or foreign agent. Note the deviation from RFC 3344: the foreign agent will not display busy or registration required information. Both are handled on a per-interface basis (see the **show ip mobile interface** command), not at the global foreign agent level.

Examples

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

```
Router# show ip mobile globals
IP Mobility global information:
Home Agent
    Registration lifetime: 10:00:00 (36000 secs)
    Broadcast enabled
    Replay protection time: 7 secs
    Reverse tunnel enabled
    ICMP Unreachable enabled
    Strip realm enabled
    NAT detect disabled
    HA Accounting enabled using method list: mylist
    Address 1.1.1.1
    Virtual networks
        10.0.0.0/8
Foreign Agent
```

```
    Pending registrations expire after 120 seconds
    Care-of address advertised
    Mobile network route injection enabled
    Mobile network route redistribution disabled
    Mobile network route injection access list mobile-net-list
    Ethernet2/2 (10.10.10.1) - up
Mobility Agent
1 interfaces providing service
Encapsulations supported: IPIP and GRE
Tunnel fast switching enabled, cef switching enabled
Discovered tunnel MTU aged out after 1:00:00
```

The following example shows that home agent UDP tunneling is enabled with a keepalive timer set at 60 seconds and forced UDP tunneling enabled.

```
Router# show ip mobile globals
IP Mobility global information:
Home agent
 Registration lifetime: 10:00:00 (36000 secs)
 Broadcast disabled
 Replay protection time: 7 secs
 Reverse tunnel enabled
 ICMP Unreachable enabled
 Strip realm disabled
 NAT Traversal disabled
 HA Accounting disabled
 NAT UDP Tunneling support enabled
 UDP Tunnel Keepalive 60
 Forced UDP Tunneling enabled
 Virtual networks
 10.99.101.0/24
Foreign agent is not enabled, no care-of address
0 interfaces providing service
Encapsulations supported: IPIP and GRE
Tunnel fast switching enabled, cef switching enabled
Tunnel path MTU discovery aged out after 10 min
```

The following example shows that NAT UDP tunneling support is enabled on the foreign agent with a keepalive timer set at 110 seconds and forced UDP tunneling disabled.

```
Router# show ip mobile globals
IP Mobility global information:
Foreign Agent
Pending registrations expire after 120 secs
Care-of addresses advertised
Mobile network route injection disabled
Ethernet2/2 (10.30.30.1) - up
1 interface providing service
Encapsulations supported: IPIP and GRE
Tunnel fast switching enabled, cef switching enabled
Tunnel path MTU discovery aged out after 10 min
NAT UDP Tunneling support enabled
UDP Tunnel Keepalive 110
Forced UDP Tunneling disabled
```

The following example output shows that multipath support is enabled:

```
Router# show ip mobile globals
IP Mobility global information:
Home Agent
    Registration lifetime: 10:00:00 (36000 secs)
    Broadcast disabled
    Replay protection time: 7 secs
    ....
    UDP Tunnel Keepalive 110
    Forced UDP Tunneling disabled
    Multiple Path Support enabled
```

The below table describes the significant fields shown in the sample output.

Table 10: show ip mobile globals Field Descriptions

Field	Description
Home Agent	
Registration lifetime	Default lifetime (in hh:mm:ss) for all mobile nodes. Number of seconds given in parentheses.
Roaming access list	Determines which mobile nodes are allowed to roam. Displayed if defined.
Care-of access list	Determines which care-of addresses are allowed to be accepted. Displayed if defined.
Broadcast	Whether broadcast is enabled or disabled.
Replay protection time	Time, in seconds, that the time stamp on a registration request (RRQ) from a mobile node may differ from the router’s internal clock.
Reverse tunnel	Whether reverse tunnel is enabled or disabled.
ICMP Unreachable	Sends ICMP unreachable messages, which are enabled or disabled for the virtual network.
Strip realm	Whether strip realm is enabled or disabled.
NAT detect	Whether NAT detect is enabled or disabled. If NAT detect is enabled, the home agent can detect a registration request that has traversed a NAT-enabled device and can apply a tunnel to reach the Mobile IP client.
HA Accounting	Whether home agent accounting is enabled or disabled.
NAT UDP Tunneling support	Whether NAT UDP tunneling is enabled or disabled on the home agent.
UDP Tunnel Keepalive	Keepalive interval, in seconds, configured on the home agent that avoids a NAT translation entry on a NAT device from expiring when there is no active Mobile IP data traffic going through the UDP tunnel.
Forced UDP Tunneling	Whether the home agent is configured to accept forced UDP tunneling.
Address	Home agent address.

Field	Description
Virtual networks	Lists virtual networks serviced by the home agent. Displayed if defined.
Multiple Path Support	Whether multiple path support is enabled or disabled.
Foreign Agent	
Pending registrations expire after	The amount of time, in seconds, before a pending registration will time out.
Care-of addresses advertised	Displayed if care-of addresses are defined.
Mobile network route injection	Mobile network route injection can be enabled or disabled.
Mobile network route redistribution	Mobile network route redistribution can be enabled or disabled.
Mobile network route injection access list	The name of the access list used if mobile network route injection is enabled.
NAT UDP Tunneling support	Whether NAT UDP tunneling is enabled or disabled on the foreign agent
UDP Tunnel Keepalive	Keepalive interval, in seconds, configured on the foreign agent that avoids a NAT translation entry on a NAT device from expiring when there is no active Mobile IP data traffic going through the UDP tunnel.
Forced UDP Tunneling	Whether the foreign agent is configured to force UDP tunneling.
up, interface-only, transmit-only	Up status is displayed if the foreign agent is configured to function in an asymmetric link environment. Interface-only status is displayed if the foreign agent is configured to advertise only its own address as the care-of address in an asymmetric link environment. Transmit-only status is displayed if the foreign agent is configured to transmit only from the interface in an asymmetric link environment.
Mobility Agent	
Number of interfaces providing service	See the **show ip mobile interface** command for more information on the interfaces providing service. Agent advertisements are sent when ICMP Router Discovery Protocol (IRDP) is enabled.

Field	Description
Encapsulations supported	The encapsulation types that are supported. Possible encapsulation types are IPIP and GRE.
Tunnel fast switching	Whether tunnel fast switching is enabled or disabled.
cef switching	Whether CEF switching is enabled or disabled.
Discovered tunnel MTU	Aged out after amount of time (in hh:mm:ss).

Related Commands

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

show ip mobile host

To display mobile node information, use the **show ip mobile host**command inprivileged EXEC mode.

show ip mobile host [*address*| **interface** *interface*| **network** *address*| **nai string**| **group** [**nai string**]| **summary**]

Syntax Description

address	(Optional) IP address of specific mobile node. If not specified, information for all mobile nodes is displayed.
interface interface	(Optional) Displays all mobile nodes whose home network is on this interface.
network address	(Optional) Displays all mobile nodes residing on this network or virtual network.
nai string	(Optional) Network access identifier.
group	(Optional) Displays all mobile node groups configured using the **ip mobile host** command.
summary	(Optional) Displays all values in the table.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2(2)XC	The nai keyword was added.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Examples

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

```
Router# show ip mobile host
10.34.253.147:
   Allowed lifetime 10:00:00 (36000/default)
   Roam status -Registered-, Home link on virtual network 10.34.253.128 /26
   Accepted 2082, Last time 02/13/03 01:03:24
   Overall service time 1w0d
   Denied 32, Last time 01/03/03 21:13:43
   Last code 'registration id mismatch (133)'
   Total violations 32
   Tunnel to MN - pkts 0, bytes 0
   Reverse tunnel from MN - pkts 0, bytes 0
```

The following is sample output from the **show ip mobile host nai***string*command:

```
Router# show ip mobile host nai
jane@cisco.com
jane@cisco.com
   Allowed lifetime 10:00:00 (36000/default)
   Roam status -Registered-, Home link on interface Loopback0
   Bindings 10.34.253.205
   Accepted 3705, Last time 02/13/03 01:02:37
   Overall service time 6d05h
   Denied 4918, Last time 01/30/03 20:59:14
   Last code 'administratively prohibited (129)'
   Total violations 262
   Tunnel to MN - pkts 0, bytes 0
   Reverse tunnel from MN - pkts 0, bytes 0
```

The below table describes the significant fields shown in the display.

Table 11: show ip mobile host Field Descriptions

Field	Description
IP address	Home IP address of the mobile node. The network access identifier (NAI) is displayed if configured.
Allowed lifetime	Allowed lifetime (in hh:mm:ss) of the mobile node. By default, it is set to the global lifetime (**ip mobile home-agent lifetime**command). Setting this lifetime will override global value.
Roaming status	When the mobile node is registered, the roaming status is - Registered - ; otherwise, it is - Unregistered -. Use the **show ip mobile binding** command for more information when the user is registered.
Home link	Interface or virtual network.
Accepted	Total number of service requests for the mobile node accepted by the home agent.
Last time	The time at which the most recent registration request was accepted by the home agent for this mobile node.
Overall service time	Overall service time that has accumulated for the mobile node since the router has booted or cleared.
Denied	Total number of service requests for the mobile node denied by the home agent (sum of all registrations denied with Code 128 through Code 159).
Last time	The time at which the most recent registration request was denied by the home agent for this mobile node.

Field	Description
Last code	The code indicating the reason why the most recent registration request for this mobile node was rejected by the home agent.
Total violations	Total number of security violations.
Tunnel to mobile node	Number of packets and bytes tunneled to mobile node.
Reverse tunnel from mobile node	Number of packets and bytes reverse tunneled from mobile node.
NAI string	NAI associated with the mobile node.
Bindings	Addresses currently assigned to the NAI.

The following is sample output from the **show ip mobile host group**command for groups configured with the **ip mobile host** command:

```
Router# show ip mobile host group
20.0.0.1 - 20.0.0.20:
    Home link on virtual network 20.0.0.0 /8, Care-of ACL -none-
    Security associations on router, Allowed lifetime 10:00:00 (36000/default)
```

The below table describes the significant fields shown in the display.

Table 12: show ip mobile host group Field Descriptions

Field	Description
IP address	Mobile host IP address or grouping of addresses.
Home link	Interface or virtual network.
Care-of ACL	Care-of address access list.
Security association	Router or AAA server.
Allowed lifetime	Allowed lifetime for mobile host or group.

Related Commands

Command	Description
clear ip mobile host-counters	Clears the mobile node counters.
show ip mobile binding	Displays the mobility binding table.

show ip mobile interface

To display advertisement information for interfaces that are providing foreign agent service or are home links for mobile nodes, use the **show ip mobile interface**command inprivilegedEXEC mode.

show ip mobile interface [*interface*]

Syntax Description

interface	(Optional) IP address of mobile node. If not specified, all interfaces are shown.

Command Modes

Privileged EXEC

Command History

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

Examples

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

```
Router# show ip mobile interface
IP Mobility interface information:
IRDP disabled
Interface Ethernet3:
    Prefix Length not advertised
    Lifetime is 36000 seconds
    Home Agent service provided
```

The below table describes the significant fields shown in the display.

Table 13: show ip mobile interface Field Descriptions

Field	Description
Interface	Name of the interface.
IRDP	IRDP (includes agent advertisement) enabled or disabled. IRDP must be enabled for an advertisement to be sent out. Use the **ip irdp** command to enable IRDP.
Prefix Length	Prefix-length extension to be included or not in the advertisement.
Lifetime	Advertised registration lifetime.

Field	Description
Home Agent service provided	Displayed if home agent service is enabled on the interface.
Foreign Agent service provided	Displayed if foreign agent service is enabled on the interface.
Registration required	Foreign agent requires registration even from those mobile nodes that have acquired their own collocated care-of address.
Busy	Foreign agent is busy for this interface.
Home Agent access list	Which home agent is allowed.
Maximum number of visitors allowed	Displayed if defined.
Current number of visitors	Number of visitors on the interface.

Related Commands

Command	Description
description (mobile networks)	Enables foreign agent service.
ip mobile host	Configures the mobile host or mobile node group.
ip mobile prefix-length	Appends the prefix-length extension to the advertisement.
show ip irdp	Displays IRDP values.

show ip mobile mobile-networks

To display a list of mobile networks associated with the mobile router, use the **show ip mobile mobile-networks**commandinprivilegedEXEC mode.

show ip mobile mobile-networks [*ip-address*]

Syntax Description

ip-address	(Optional) Address of a specific mobile router. If not specified, information for all mobile networks is displayed.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.2(13)T	This command was enhanced to display information about the dynamically registered mobile networks.
12.4(9)T	This command was enhanced to display information about multipath support.

Usage Guidelines

The home agent maintains a list of static and dynamic mobile networks associated with mobile routers.

Examples

The following is sample output from the **show ip mobile mobile-networks** command:

```
Router# show ip mobile mobile-networks
Mobile Networks:
MR 20.0.4.1:
Dynamic registration
    Configured:10.2.0.0/255.255.255.0
    Registered:10.3.0.0/255.255.255.0
               10.4.0.0/255.0.0.0
               10.5.0.0/255.255.255.0
```

The following is sample output from the **show ip mobile mobile-networks** command when multipath support is enabled:

```
Router# show ip mobile mobile-networks
Mobile Networks:
MR 10.1.1.1:
    Multiple Paths Support Enabled
    Dynamic registration
    Registered:10.2.0.0/255.255.255.0
```

The below table describes the significant fields in the display.

Table 14: show ip mobile mobile-networks Field Descriptions

Field	Description
MR	IP address of the mobile router.
Multiple Paths Support Enabled	Configured for multiple path support between the mobile router and the home agent.
Dynamic registration	Configured for dynamic registration of mobile networks.
Configured	Mobile networks statically configured on the home agent.
Registered	Mobile networks dynamically registered on the home agent.

Related Commands

Command	Description
ip mobile mobile-networks	Associates one or more networks with a mobile router configured as a mobile host and enters mobile networks configuration mode.

show ip mobile proxy

To display information about a proxy Mobile IP host, use the **show ip mobile proxy**command in privileged EXEC mode.

show ip mobile proxy [**host** [**nai** *string*]]| **registration**| **traffic**]

Syntax Description

host	(Optional) Displays information about the proxy host.
nai *string*	(Optional) Network access identifier.
registration	(Optional) Displays proxy registration information.
traffic	(Optional) Displays proxy traffic information.

Command Modes

Privileged EXEC

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 PDSN platforms.

Usage Guidelines

This command is available only on Packet Data Serving Node (PDSN) platforms running specific PDSN code images; consult Feature Navigator for your Cisco IOS software release.

Examples

The following is sample output from the **show ip mobile proxy host**command:

```
Router# show ip mobile proxy host
Proxy Host List:
MoIPProxy1@cisco.com:
    Home Agent Address 10.3.3.1
    Lifetime 6000
    Flags :sBdmgvt
```

show ip mobile router

To display configuration information and monitoring statistics about the mobile router, use the **show ip mobile router** command in privileged EXEC mode.

show ip mobile router

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.2(13)T	This command was enhanced to display information about the mobile network interfaces.
12.2(15)T	This command was enhanced to display information about collocated care-of addresses (CCoAs).
12.3(7)T	This command was enhanced to display information about requests for generic routing encapsulation (GRE).
12.4(9)T	The command was enhanced to display information about multipath support.

Usage Guidelines

The display includes the mobile router configuration information such as the home address and network mask, home agent, and registration settings, and operational information such as status, tunnel interface, active foreign agent, and care-of address.

Examples

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

```
Router# show ip mobile router
Mobile Router
  Enabled 05/30/02 11:16:03
  Last redundancy state transition 05/30/02 11:15:01
Configuration:
  Home Address 10.0.4.1 Mask 255.255.255.0
  Home Agent 10.0.0.3 Priority 100 (best) (current)
  Registration lifetime 120 sec
  Retransmit Init 1000, Max 5000 msec, Limit 3
  Extend Expire 120, Retry 3, Interval 10
  Redundancy group AlwaysUp (active)
  Mobile Networks:Ethernet5 (10.0.0.0/255.255.255.248)
    Ethernet2 (10.0.0.0/255.0.0.0)
    Ethernet3 (10.1.0.0/255.255.255.0)
Monitor:
  Status -Registered-
  Active foreign agent 10.0.1.2, Care-of 10.0.1.2
  On interface Serial0
  Tunnel0 mode IP/IP
```

The following is sample output from the **show ip mobile router**command when a mobile router is registered using a CCoA:

```
Router# show ip mobile router
Mobile Router
  Enabled 02/12/02 18:29:13
  Last redundancy state transition NEVER
Configuration:
  Home Address 10.0.4.1 Mask 255.255.255.0
  Home Agent 10.0.0.3 Priority 100 (best)
  Registration lifetime 120 sec
  Retransmit Init 1000, Max 5000 msec, Limit 3
  Extend Expire 120, Retry 3, Interval 10
Monitor:
  Status -Registered-
  Using Collocated Care-of Address 10.0.0.1
  On interface Ethernet1
  Tunnel0 mode IP/IP
```

The following is sample output from the **show ip mobile router**command when GRE encapsulation is globally configured on the mobile router. When GRE encapsulation is enabled, the line “Request GRE tunnel” is displayed in the output and the tunnel mode is shown as “GRE/IP.”

```
Router# show ip mobile router
Mobile Router
    Enabled 01/11/00 06:59:19
    Last redundancy state transition NEVER
Configuration:
    Home Address 10.80.80.1 Mask 255.255.255.0
    Home Agent 10.40.40.1 Priority 100 (best) (current)
    Registration lifetime 65534 sec
    Retransmit Init 1000, Max 5000 msec, Limit 3
    Extend Expire 20, Retry 10, Interval 1
    Request GRE tunnel
    Mobile Networks:Ethernet1/3 (172.16.143.0/255.255.255.0)
                     TokenRing4/3 (172.16.153.0/255.255.255.0)
Monitor:
    Status -Registered-
    Active foreign agent 10.52.52.1, Care-of 10.52.52.1
    On interface TokenRing4/2
    Tunnel0 mode GRE/IP
```

The following is sample output when the mobile router is configured for multipath support:

```
Router# show ip mobile router
Mobile Router
    Enabled 11/22/05 05:37:17
    Last redundancy state transition NEVER
Configuration:
    Home Address 10.1.1.10 Mask 255.255.255.0
    Home Agent 10.1.1.2 Priority 100 (best) (current)
    Registration lifetime 90 sec
    Retransmit Init 1000, Max 5000 msec, Limit 3
    Extend Expire 120, Retry 3, Interval 10
    Reverse tunnel required
    Multi-path active, Requested metric: bandwidth, Using metric: bandwidth
    Mobile Networks: Ethernet3/0 (172.16.1.0/255.255.255.0)
                     Loopback44 (192.168.1.0/255.255.255.0)
Monitor:
    Status -Registered-
    Foreign Agent 172.20.1.1, Care-of 172.20.1.1
         On interface Ethernet1/0
         Tunnel0 mode IP/IP
    Collocated care-of address 172.30.1.11
         On interface Ethernet2/0
         Tunnel2 mode IP/IP
    Collocated care-of address 172.40.1.11
```

```
        On interface Ethernet3/0
        Tunnel3 mode GRE/IP
```

The below table describes the significant fields shown in the display.

Table 15: show ip mobile router Field Descriptions

Field	Description
Enabled	Date and time (in hh:mm:ss) when the mobile router was enabled.
Last redundancy state transition	Date and time (in hh:mm:ss) when the redundancy state of the mobile router changed.
Home Address/Mask	Home IP address of the mobile router, including the network mask.
Home Agent	Home agent that the mobile router registers with. The mobile router registers only to the home agent with the highest priority when multiple addresses are configured.
Registration lifetime	Registration lifetime (in seconds) granted by the home agent for the mobile router.
Retransmit Init/Max/Limit	Registration request retransmission settings. When registration requests are not responded to, the mobile router will resend. Displays the initial and maximum transmission timers and the limit on the number of retries allowed.
Extend Expire/ Retry/Interval	Extend registration lifetime. After the mobile router has registered, reregister before the lifetime expires. Retry is the number of attempts to reregister between intervals.
Request GRE tunnel	The mobile router requests GRE encapsulation when it registers.
Redundancy group	Name of the redundancy group used to provide mobile router redundancy. Mobile router is either “active” or “passive.” If redundancy is enabled or disabled, this information is displayed or absent, respectively. Active means that the mobile router is functioning fully, and passive means that the mobile router is idle.
Reverse tunnel required	If reverse tunnel is enabled or disabled, this information is displayed or absent, respectively.
Multi-path active	Multiple path support is active between the mobile router and the home agent.

Field	Description
Multi-path enabled	Multiple path support is enabled, but the mobile router is not registered yet.
Multi-path denied by HA	Multiple path support is disabled on the home agent.
Requested metric: bandwidth	Requested metric to use to load balance traffic among multiple paths. The metric is either bandwidth or hop count. Bandwidth is the default.
Using metric: bandwidth	Metric that is being used to load balance traffic among multiple paths. The metric is either bandwidth or hopcount. Bandwidth is the default.
Mobile Networks	Mobile networks associated with the mobile router.
Status	Indication of the state of the mobile router. Options are as follows: • Home--Connected to home network. • Registered--Registered on foreign network. • Pending--Sent registration and waiting for reply. • Isolated--Mobile router has heard an agent advertisement but is isolated from the network. • Unknown--Cannot determine status.
Active foreign agent/Care-of	Foreign agent and care-of address used by the registered mobile router.
Using Collocated Care-of Address	Displayed if a mobile router is registered using a CCoA.
On interface	Mobile router registered on this interface.
Tunnel	Tunnel number between mobile router and the home agent.
mode	The type of encapsulation being used. The encapsulation type can be one of the following: • GRE/IP--GRE encapsulation is being used. • IP/IP--IP-in-IP encapsulation is being used.

Related Commands

Command	Description
ip mobile router	Enables the mobile router and enters mobile router configuration mode.

show ip mobile router agent

To display information about the agents for the mobile router, use the **show ip mobile router agent** command inprivilegedEXEC mode.

show ip mobile router agent

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.2(15)T	This command was enhanced to display information about the retry interval used in static collocated care-of address (CCoA) processing.
12.3(4)T	This command was enhanced to display information about dynamic CCoA processing.
12.3(14)T	This command was enhanced to display the default gateway for dynamic CCoA acquired through DHCP.

Usage Guidelines

This command displays a list containing information on all foreign agents currently discovered on the mobile router. This list also displays information about each interface configured for static or dynamic CCoA. An interface must be “up” to be displayed on the list.

You can use the **clear ip mobile router agent** command to clear foreign agent care-of addresses (CoAs) but not static CCoAs. CCoAs cannot be cleared.

Examples

The following is sample output from the **show ip mobile router agent**command when a CCoA is configured on a mobile router interface:

```
Router# show ip mobile router agent
Mobile Router Agents:
Foreign agent 45.0.0.2:
  Care-of address 42.0.0.2
  Interface Ethernet1, MAC 0030.9492.6627
  Agent advertisement seq 56649, Flags rbhFmGvt, Lifetime 36000
  IRDP advertisement lifetime 30, Remaining 29
  Last received 02/13/02 17:55:48
  First heard 02/13/02 11:21:46
Collocated Care-of address 48.0.0.1 (static):
  Interface Ethernet2
  Default gateway 48.0.0.2
  Registration retry interval 60
  Next CCoA reg attempt in 00:00:55 seconds
Collocated Care-of address 11.0.0.7 (dynamic):
  Interface Serial0
  Registration retry interval 60
```

The below table describes the significant fields shown in the display.

Table 16: show ip mobile router agent Field Descriptions

Field	Description
Home or Foreign Agent	IP address of the foreign agent (or home agent).
Care-of address	Attachment point in the foreign network.
Interface	Interface on which the agent was learned.
MAC	MAC address of the learned agent.
Agent advertisement seq/Flags/Lifetime	Agent advertisement sequence number, flags, and lifetime (in seconds). The sequence number can be used to detect reboot by the agent. The flags are services provided by the agent. The lifetime is the limit advertised by the agent.
IRDP advertisement lifetime/Remaining	The IRDP advertisement lifetime is the interval in which this foreign agent will provide service. When the lifetime expires, the foreign agent is disconnected from the mobile router. The remaining field shows the time before expiration.
Last received	Date and time when advertisement was received.
First heard	Date and time when the agent was first heard. This is useful information in determining which agent to use when multiple learned agents are heard by the mobile router.
Collocated Care-of address	CCoA configured on the mobile router interface. The type of CCoA (static or dynamic) is given in parentheses.
Interface	Mobile router interface.
Default gateway	The next-hop IP address for registration packets. Upon successful registration, this address will be used as the default gateway and default route. This field is displayed if the IP address is fixed (static) on an Ethernet interface or a default gateway is acquired through DHCP.

Field	Description
Registration retry interval	The interval that the mobile router waits before sending another registration request if a registration request failed.
Next CCoA reg attempt in 00:00:55 seconds	If the interval timer is running, the time remaining (in seconds) until the next registration attempt. Only appears if a registration attempt (and its retries) has failed and the registration retry interval timer is running.

Related Commands

Command	Description
clear ip mobile router agent	Deletes learned agents and the corresponding care-of address of the foreign agent from the mobile router agent table.

show ip mobile router interface

To display information about the interfaces configured for roaming, use the **show ip mobile router interface** command in privileged EXEC mode.

show ip mobile router interface

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.2(15)T	This command was enhanced to display information about static collocated care-of addresses (CCoAs).
12.3(4)T	This command was enhanced to display information about dynamic CCoAs.
12.3(7)T	This command was enhanced to display information about a request for a generic routing encapsulation (GRE) tunnel.
12.3(14)T	This command was enhanced to display information about Layer 2 signaling on roaming interfaces.

Usage Guidelines

The mobile router uses the interfaces for roaming, discovering foreign agents, and registering its location on the foreign network.

Use this command to display information about roaming interfaces. If the interface is configured for a collocated care-of address (CCoA), the CCoA IP address is displayed. If it is not configured for a CCoA, “disabled” is displayed. The interface can be up or down.

Examples

The following is sample output from the **show ip mobile router interface** command. Fast Ethernet interface 0/0 and Fast Ethernet interface 2/0 have no CCoA configuration, serial interface 1/0 has a static CCoA configuration, and serial interface 1/1 has a dynamic CCoA address with CCoA only. GRE encapsulation is configured on Fast Ethernet interface 2/0.

```
Router# show ip mobile router interface
Mobile Router Interfaces:
Listed in order of preference.
FastEthernet0/0:
  Priority 102, Bandwidth 10000, Address 10.0.0.9
  Periodic solicitation disabled, Interval 600 sec
  Retransmit Init 1000, Max 5000 msec, Limit 3
  Current 0, Remaining 0 msec, Count 0
  Hold down 0 sec
  Routing disallowed
  Collocated CoA disabled
Serial1/0:
  Priority 100, Bandwidth 1544, Address 10.0.0.7
  Periodic solicitation disabled, Interval 600 sec
  Retransmit Init 1000, Max 5000 msec, Limit 3
  Current 1000, Remaining 0 msec, Count 1
  Hold down 0 sec
  Routing disallowed
  Collocated CoA 10.0.0.7 (static)
Serial1/1
  Priority 100, Bandwidth 1544, Address 10.0.0.5
  Periodic solicitation disabled, Interval 600 sec
  Retransmit Init 1000, Max 5000 msec, Limit 3
  Current 0, Remaining 0 msec, Count 0
  Hold down 0 sec
  Routing disallowed
  Collocated CoA 10.0.0.5 - Solicit FA first
FastEthernet2/0
  Priority 110, Bandwidth 16000, Address 10.52.52.2
  Periodic solicitation disabled, Interval 600 sec
  Retransmit Init 1000, Max 5000 msec, Limit 3
  Current 2000, Remaining 0 msec, Count 2
  Hold down 0 sec
  Routing disallowed
  Collocated CoA disabled
  Request GRE tunnel
```

The following sample output shows that the mobile router is configured to support signaling on roaming interfaces via SNMP interface MIB traps.

```
Router# show ip mobile router interface
Mobile Router Interfaces:
Listed in order of preference.
Ethernet1:
  Priority 110, Bandwidth 10000, Address 55.0.0.8
  Periodic solicitation disabled, Interval 600 sec
  Retransmit Init 1000, Max 5000 msec, Limit 3
  Current 5000, Remaining 0 msec, Count 4
  Foreign agent hold down 0 sec
  Layer 2 reassociation hold down 5000 msec
  Last layer 2 link-state trap: linkDown
  Routing disallowed
  Collocated CoA 55.0.0.8 - Solicit FAs
```

The below table describes the significant fields shown in the display.

Table 17: show ip mobile router interface Field Descriptions

Field	Description
Priority	Interface priority. Comparison to decide the preferred interface to register by the mobile router. The interface with the highest priority is used to send registrations.
Bandwidth	Interface bandwidth. When multiple interfaces have the highest priority, the highest bandwidth is the preferred choice.
Address	Interface IP address. If priority and bandwidth are the same among roaming interfaces, the highest address is preferred by the mobile router.

Field	Description
Periodic solicitation	Send solicitations periodically (enabled) or wait for periodic advertisements (disabled).
Interval	Period of time (in seconds) to wait before sending the next periodic solicitation.
Retransmit Init/Max/Limit	Solicitation retry settings. Displays the initial and maximum transmission timers and the limit on the number of retries allowed.
Current/ Remaining	Current retransmission interval and remaining time (in milliseconds) before it expires.
Count	Retransmission count.
Hold down	Period of time (in seconds) to wait before registering to a learned agent.
Layer 2 reassociation hold down	Period of time (in milliseconds) that the mobile router will wait for an SNMP linkUp trap from the WMIC indicating that the wireless link is available for use.
Last layer 2 link-state trap	The last layer 2 linkDown and linkUp trap events signaled via SNMP.
Routing	Routing is disallowed when the mobile router is roaming and allowed when the mobile router is home.
Collocated CoA	IP address is displayed if the interface is configured for CCoA; otherwise “Collocated CoA disabled” is displayed. The CCoA is displayed if configured, even if the interface is down. The type of CCoA (static or dynamic) is given in parentheses.
Solicit FA first	Interface will solicit foreign agents first. If none are heard, CCoA processing is enabled on the interface.
Request GRE tunnel	Interface will request GRE encapsulation when it registers with an agent.

Related Commands

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

Command	Description
keepalive	Enables keepalive packets and specifies the number of times that the Cisco IOS software tries to send keepalive packets without response before bringing the tunnel protocol down for a specific interface.

show ip mobile router registration

To display pending and/or accepted registrations of the mobile router, use the **show ip mobile router registration**command inprivilegedEXEC mode.

show ip mobile router registration

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.2(13)T	This command was enhanced to display new extensions in the registration request.
12.2(15)T	This command was enhanced to display collocated care-of addresses (CCoAs) if configured.

Examples

The following is sample output from the **show ip mobile router registration** command:

```
Router# show ip mobile router registration
Mobile Router Registrations:
Foreign Agent 44.0.0.1:
  Registration accepted 01/15/01 10:04:01, On Ethernet2/2
  Care-of addr 41.0.0.1, HA addr 49.0.0.3, Home addr 49.0.0.5
  Lifetime requested 01:00:00 (3600), Granted 00:30:00 (1800)
  Remaining 00:20:13
  Flags sbdmgvt, Identification BE0D49E5.5E1C56E4
  Register next time 00:18:13
  Extensions
    Mobile Network 44.0.0.0/8
    MN-HA Authentication SPI 100
```

The following is sample output from the **show ip mobile router registration** command if a mobile router interface is configured with a CCoA:

```
Home agent 4.4.4.3:
  Registration accepted 01/01/02 10:24:46, On Ethernet5/3
  Collocated care-of addr 3.3.3.2, HA addr 4.4.4.3, Home addr 4.4.4.2
  Lifetime requested 00:01:30 (90), Granted 00:01:30 (90)
  Remaining 00:01:08
  Flags sbDmg-T-, Identification BFDC0CEE.C7A75D64
  Register next time 00:00:23
  Extensions:
    Mobile Network 95.95.95.0/24
    MN-HA Authentication SPI 100
```

The below table describes the significant fields shown in the display.

Table 18: show ip mobile router registration Field Descriptions

Field	Description
Home or Foreign Agent	IP address of the home agent or foreign agent.
Registration accepted	Date and time (in hh:mm:ss) when registration was accepted.
On	Which interface registration occurred on.
Care-of addr/Collocated care-of addr	Attachment point in the foreign network. The collocated care-of address is displayed if configured.
HA addr	IP address of the home agent.
Home addr	Home IP address.
Lifetime requested	Requested lifetime of registration.
Granted	Registration lifetime granted by the home agent.
Remaining	Remaining time before registration expires.
Flags	Flags in the registration reply.
Identification	Identification in the registration reply.
Register next time	Remaining time before the mobile router sends the next registration request.
Extensions	New extensions added to the registration request.
Mobile Network	Mobile network connected to mobile router.
MN-HA Authentication	Mobile node and home agent authentication. Indicates the SPI number.

Related Commands

Command	Description
register (mobile router)	Controls the registration parameters of the mobile router.

show ip mobile router traffic

To display the counters that the mobile router maintains, use the **show ip mobile router traffic**command in privileged EXEC mode.

show ip mobile router traffic [**since bootup**]

Syntax Description

since bootup	(Optional) Displays counters since the mobile router process started, regardless of how many times the counters were cleared.

Command Default

Displays counters since the counters were last cleared.

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

The mobile router maintains counters for agent discovery, registration, movement, and services.

Examples

The following is sample output from the **show ip mobile router traffic**command:

```
Router# show ip mobile router traffic
Mobile Router Counters:
Agent Discovery:
  Solicitations sent 90, advertisements received 17
  Agent reboots detected 0
Registrations:
  Register 70, Deregister 0 requests sent
  Register 70, Deregister 0 replies received
  Requests accepted 68, denied 1 by HA 1 /FA 0
  Denied due to mismatched ID 1
  Authentication failed for HA 0/FA 0
  Invalid extensions 0, ignored 0
  Invalid home address 0, ID 0
  Unknown HA 0/FA 0
  Gratuitous ARPs sent 0
Movement:
  Came up on HA 0, on FA 1
  Moved HA to FA 0, FA to FA 0, FA to HA 0
  Better interface detected 0 source 46.0.0.5 dest 49.0.0.3
Tunnel Traffic:
  Packets received 188105, sent 0
  Bytes received 142691351, sent 0
Services:
  Redundancy state active 2, passive 1
```

The below table describes the significant fields shown in the display.

Table 19: show ip mobile router traffic Field Descriptions

Field	Description
Agent Discovery	Counters categorized for discovering agents.
Solicitations sent	Total number of solicitations sent by the mobile router.
Advertisements received	Total number of advertisements received by the mobile router.
Agent reboots detected	Total number of agent reboots detected by the mobile router through the sequence number of the advertisement.
Registrations	Counters categorized for registration.
Register / Deregister requests sent	Total number of registration and deregistration requests sent by the mobile router.
Register / Deregister replies received	Total number of registration and deregistration replies received by the mobile router.
Requests accepted	Total number of registration requests accepted by the home agent of the mobile router (Code 0 and Code 1).
denied by HA/FA	Total number of registration requests denied by the home agent of the mobile router (sum of Code 128 through Code 191) and visited foreign agent (sum of Codes 64 through Code 127).
Denied due to mismatched ID	Total number of registration requests denied by the home agent due to identification mismatch. This means that the mobile router needs to synchronize its clock with the home agent in its request. A mobile router will adjust its time in the identification field to match the home agent's time for subsequent requests.
Authentication failed for HA/FA	Total number of authentication failures.
Invalid extensions	Total number of registration replies dropped by the mobile router due to both poorly formed extensions and unrecognized extensions with extension number in the range from 0 to 127.

Field	Description
Invalid ignored	Total number of registration replies that contained one or more unrecognized extensions in the range from 128 to 255 that were ignored by the mobile router.
Invalid home address	Total number of replies with an invalid home address.
Invalid ID	Total number of replies with an invalid Identification field.
Unknown HA/FA	Total number of replies with unknown home agents or foreign agents.
Gratuitous ARPs sent	Total number of Gratuitous ARPs sent by the mobile router in order to clear out any stale ARP entries in the ARP caches of nodes on the home network.
Movement	Counters categorized for movement.
Came up on HA/on FA	Number of times the mobile router came up on its home network or some foreign network.
Moved HA to FA / FA to FA / FA to HA	Number of times that the mobile router moved between its home network and the foreign network, and among foreign networks.
Better interface detected	Number of times a better interface was detected.
Tunnel Traffic	Counters categorized for tunnel traffic while the mobile router is roaming.
Packets received / sent	Number of packets received and sent by the mobile router.
Bytes received / sent	Number of bytes received and sent by the mobile router.
Services:	Mobile router services.
Redundancy state active <2>, passive <1>	Number of times the mobile router changes between active and passive states, which occurs when a redundancy state change is detected.

Related Commands

Command	Description
clear ip mobile router traffic	Clears the counters that the mobile router maintains.

show ip mobile secure

To display the mobility security associations for the mobile host, mobile visitor, foreign agent, home agent, or proxy Mobile IP host, use the **show ip mobile secure**command in privileged EXEC mode.

show ip mobile secure {**host**| **visitor**| **foreign-agent**| **home-agent**| **proxy-host**| **summary**} {*ip-address*| **nai string**}

Syntax Description

host	Displays security association of the mobile host on the home agent.
visitor	Displays security association of the mobile visitor on the foreign agent.
foreign-agent	Displays security association of the remote foreign agents on the home agent.
home-agent	Displays security association of the remote home agent on the foreign agent.
proxy-host	Displays security association of the proxy mobile user. This keyword is only available on Packet Data Serving Node (PDSN) platforms running specific PDSN code images.
summary	Displays number of security associations in table.
ip-address	IP address.
nai *string*	Network access identifier (NAI).

Command Modes

EXEC

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2(2)XC	The nai keyword was added.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.3(4)T	The **proxy-host** keyword was added for PDSN platforms.

Usage Guidelines

Multiple security associations can exist for each entity.

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

Examples

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

```
Router# show ip mobile secure
Security Associations (algorithm,mode,replay protection,key):
10.0.0.6
    SPI 300,  MD5, Prefix-suffix, Timestamp +/- 7,
    Key 00112233445566778899001122334455
```

The below table describes the significant fields shown in the display.

Table 20: show ip mobile secure Field Descriptions

Field	Description
10.0.0.6	IP address. The NAI is displayed if configured.
In/Out SPI	The SPI is the 4-byte opaque index within the mobility security association that selects the specific security parameters to be used to authenticate the peer. Allows either “SPI” or “In/Out SPI.” The latter specifies an inbound and outbound SPI pair. If an inbound SPI is received, then outbound SPI will be used when a response is sent.
MD5	Message Digest 5 authentication algorithm. HMAC-MD5 id displayed if configured.
Prefix-suffix	Authentication mode.
Timestamp	Replay protection method.
Key	The shared secret key for the security associations, in hexadecimal format.

show ip mobile traffic

To display protocol counters, use the **show ip mobile traffic**command in privileged EXEC mode.

show ip mobile traffic

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2(13)T	This command was enhanced to display successful registration requests with NAT detect and to display information about foreign agent reverse tunnels and foreign agent challenge and response extensions.
12.3(14)T	The command output was enhanced to display the count of UDP Port 434 input packets that were dropped by UDP.

Usage Guidelines

Counters can be reset to zero using the **clear ip mobile traffic**command, which also allows you to undo the reset.

Examples

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

```
Router# show ip mobile traffic
IP Mobility traffic:
UDP:
    Port: 434 (Mobile IP) input drops: 0
Advertisements:
    Solicitations received 0
    Advertisements sent 0, response to solicitation 0
Home Agent Registrations:
    Register 0, Deregister 0 requests
    Register 0, Deregister 0 replied
    Accepted 0, No simultaneous bindings 0
    Denied 0, Ignored 0
    Unspecified 0, Unknown HA 0
    Administrative prohibited 0, No resource 0
    Authentication failed MN 0, FA 0
    Bad identification 0, Bad request form 0
    Unavailable encap 0, reverse tunnel 0
    Reverse tunnel mandatory 0
    Binding updates received 0, sent 0 total 0 fail 0
    Binding update acks received 0, sent 0
    Binding info request received 0, sent 0 total 0 fail 0
    Binding info reply received 0 drop 0, sent 0 total 0 fail 0
    Binding info reply acks received 0 drop 0, sent 0
    Gratuitous 0, Proxy 0 ARPs sent
    Total incoming requests using NAT detect 1
Foreign Agent Registrations:
    Request in 0,
    Forwarded 0, Denied 0, Ignored 0
    Unspecified 0, HA unreachable 0
    Administrative prohibited 0, No resource 0
    Bad lifetime 0, Bad request form 0
    Unavailable encapsulation 0, Compression 0
    Unavailable reverse tunnel 0
    Reverse tunnel mandatory
    Replies in 0
    Forwarded 0, Bad 0, Ignored 0
    Authentication failed MN 0, HA 0
    Received challenge/gen. authentication extension, feature not enabled 0
    Route Optimization Binding Updates received 0, acks sent 0 neg acks sent 0
    Unknown challenge 1, Missing challenge 0, Stale challenge 0
```

The below table describes the significant fields shown in the display.

Table 21: show ip mobile traffic Field Descriptions

Field	Description
Port: 434 (Mobile IP) input drops	Total number of UDP Port 434 (Mobile IP) packets dropped by UDP processing due to a full input queue. These packets are not processed by the home agent or foreign agent and so are not otherwise counted or displayed by Mobile IP. This count is the same count displayed by using the **show ip socket detail** command.
Solicitations received	Total number of solicitations received by the mobility agent.
Advertisements sent	Total number of advertisements sent by the mobility agent.
response to solicitation	Total number of advertisements sent by the mobility agent in response to mobile node solicitations.
Home Agent	
Register requests	Total number of registration requests received by the home agent.
Deregister requests	Total number of registration requests received by the home agent with a lifetime of zero (requests to deregister).
Register replied	Total number of registration replies sent by the home agent.
Deregister replied	Total number of registration replies sent by the home agent in response to requests to deregister.
Accepted	Total number of registration requests accepted by the home agent (Code 0).

Field	Description
No simultaneous bindings	Total number of registration requests accepted by the home agent--simultaneous mobility bindings unsupported (Code 1).
Denied	Total number of registration requests denied by the home agent.
Ignored	Total number of registration requests ignored by the home agent.
Unspecified	Total number of registration requests denied by the home agent--reason unspecified (Code 128).
Unknown HA	Total number of registration requests denied by the home agent--unknown home agent address (Code 136).
Administrative prohibited	Total number of registration requests denied by the home agent--administratively prohibited (Code 129).
No resource	Total number of registration requests denied by the home agent--insufficient resources (Code 130).
Authentication failed MN	Total number of registration requests denied by the home agent--mobile node failed authentication (Code 131).
Authentication failed FA	Total number of registration requests denied by the home agent--foreign agent failed authentication (Code 132).
Bad identification	Total number of registration requests denied by the home agent--identification mismatch (Code 133).
Bad request form	Total number of registration requests denied by the home agent--poorly formed request (Code 134).
Unavailable encap	Total number of registration requests denied by the home agent--unavailable encapsulation (Code 139).
Reverse tunnel mandatory	Total number of registration requests denied by the home agent--reverse tunnel is mandatory and the “T” bit is not set (Code 138).
Unavailable reverse tunnel	Total number of registration requests denied by the home agent--reverse tunnel unavailable (Code 137).

Field	Description
Binding updates	A Mobile IP standby message sent from the active router to the standby router when a registration request comes into the active router.
Binding update acks	A Mobile IP standby message sent from the standby router to the active router to acknowledge the reception of a binding update.
Binding info request	A Mobile IP standby message sent from a router coming up from reboot/or a down interface. The message is a request to the current active router to send the entire Mobile IP binding table.
Binding info reply	A reply from the active router to the standby router that has part or all of the binding table (depending on size).
Binding info reply acks	An acknowledge message from the standby router to the active router that it has received the binding info reply.
Gratuitous ARP	Total number of gratuitous ARPs sent by the home agent on behalf of mobile nodes.
Proxy ARPs sent	Total number of proxy ARPs sent by the home agent on behalf of mobile nodes.
Total incoming registration requests...	Total number incoming registration requests using NAT detect.
Foreign Agent	
Request in	Total number of registration requests received by the foreign agent.
Forwarded	Total number of registration requests relayed to the home agent by the foreign agent.
Denied	Total number of registration requests denied by the foreign agent.
Ignored	Total number of registration requests ignored by the foreign agent.
Unspecified	Total number of registration requests denied by the foreign agent--reason unspecified (Code 64).

Field	Description
HA unreachable	Total number of registration requests denied by the foreign agent--home agent unreachable (Codes 80-95).
Administrative prohibited	Total number of registration requests denied by the foreign agent-- administratively prohibited (Code 65).
No resource	Total number of registration requests denied by the home agent--insufficient resources (Code 66).
Bad lifetime	Total number of registration requests denied by the foreign agent--requested lifetime too long (Code 69).
Bad request form	Total number of registration requests denied by the home agent--poorly formed request (Code 70).
Unavailable encapsulation	Total number of registration requests denied by the home agent--unavailable encapsulation (Code 72).
Unavailable compression	Total number of registration requests denied by the foreign agent--requested Van Jacobson header compression unavailable (Code 73).
Unavailable reverse tunnel	Total number of registration requests denied by the home agent--reverse tunnel unavailable (Code 74).
Reverse tunnel mandatory	Total number of registration requests denied by the foreign agent--reverse tunnel is mandatory and the “T” bit is not set (Code 75).
Replies in	Total number of well-formed registration replies received by the foreign agent.
Forwarded	Total number of valid registration replies relayed to the mobile node by the foreign agent.
Bad	Total number of registration replies denied by the foreign agent--poorly formed reply (Code 71).
Ignored	Total number of registration replies ignored by the foreign agent.
Authentication failed MN	Total number of registration requests denied by the home agent--mobile node failed authentication (Code 67).
Authentication failed HA	Total number of registration replies denied by the foreign agent--home agent failed authentication (Code 68).

Field	Description
Received challenge/gen. authentication extension, feature not enabled	Total number of registration requests dropped by the foreign agent--received challenge/generalized-authentication extension in registration request but Mobile IP foreign agent challenge/response extension is not enabled.
Unknown challenge	Total number of registration requests denied by the foreign agent--unknown challenge (Code 104).
Missing Challenge	Total number of registration requests denied by the foreign agent--missing challenge (Code 105).
Stale Challenge	Total number of registration requests denied by the foreign agent--stale challenge (Code 106).

show ip mobile tunnel

To display active tunnels, use the **show ip mobile tunnel**commandinEXEC mode.

show ip mobile tunnel [*interface*]

Syntax Description

interface	(Optional) Displays a particular tunnel interface. The *interface* argument is tunnel *x*.

Command Modes

EXEC

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2(13)T	The output was enhanced to display route maps configured on the home agent.
12.2(15)T	The output was enhanced to display tunnel templates for multicast configured on the home agent or mobile router.
12.3(8)T	The output was enhanced to display UDP tunneling.
12.4(9)T	The command was enhanced to display information about multipath support.

Usage Guidelines

This command displays active tunnels created by Mobile IP. When no more users are on the tunnel, the tunnel is released.

Examples

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

```
Router# show ip mobile tunnel
Mobile Tunnels:
Tunnel0:
 src 10.0.0.32, dest 10.0.0.48
 encap IP/IP, mode reverse-allowed, tunnel-users 1
 IP MTU 1480 bytes
 HA created, fast switching enabled, ICMP unreachable enabled
 0 packets input, 0 bytes, 0 drops
 1591241 packets output, 1209738478 bytes
 Route Map is: MoIPMap
Running template configuration for this tunnel:
ip pim sparse-dense-mode
```

The following is sample output from the show ip mobile tunnel command that verifies that UDP tunneling is established:

```
Router# show ip mobile tunnel
Mobile Tunnels:
Total mobile ip tunnels 1
Tunnel0:
    src 10.30.30.1, dest 10.10.10.100
    src port 434, dest port 434
    encap MIPUDP/IP, mode reverse-allowed, tunnel-users 1
    IP MTU 1480 bytes
    Path MTU Discovery, mtu: 0, ager: 10 mins, expires: never
    outbound interface Ethernet2/3
    FA created, fast switching disabled, ICMP unreachable enabled
    5 packets input, 600 bytes, 0 drops
    7 packets output, 780 bytes
```

The following is sample output from the show ip mobile tunnel command that shows that the mobile node-home agent tunnel is still IP-in-IP, but that the foreign agent-home agent tunnel is UDP:

```
Router# show ip mobile tunnel
Mobile Tunnels:
Total mobile ip tunnels 2
Tunnel0:
 src 10.2.1.1, dest 10.99.100.2
 encap IP/IP, mode reverse-allowed, tunnel-users 1
 IP MTU 1460 bytes
 Path MTU Discovery, mtu: 0, ager: 10 mins, expires: never
 outbound interface Tunnel1
 HA created, fast switching enabled, ICMP unreachable enabled
 11 packets input, 1002 bytes, 0 drops
 5 packets output, 600 bytes
Tunnel1:
 src 10.2.1.1, dest 100.3.1.5
 src port 434, dest port 434
 encap MIPUDP/IP, mode reverse-allowed, tunnel-users 1
 IP MTU 1480 bytes
 Path MTU Discovery, mtu: 0, ager: 10 mins, expires: never
 outbound interface GigabitEthernet0/2
 HA created, fast switching disabled, ICMP unreachable enabled
 11 packets input, 1222 bytes, 0 drops
 7 packets output, 916 bytes
```

The following is sample output from the show ip mobile tunnel command that shows that the mobile node has UDP tunneling established with the home agent:

```
Router# show ip mobile tunnel
Total mobile ip tunnels 1
Tunnel0:
 src 10.10.10.100, dest 10.10.10.50
 src port 434, dest port 434
 encap MIPUDP/IP, mode reverse-allowed, tunnel-users 1
 IP MTU 1480 bytes
 Path MTU Discovery, mtu: 0, ager: 10 mins, expires: never
 outbound interface Ethernet2/1
 HA created, fast switching disabled, ICMP unreachable enabled
 5 packets input, 600 bytes, 0 drops
 5 packets output, 600 bytes
```

The following is sample output when the mobile router is configured for multipath support:

```
Router# show ip mobile tunnel
Mobile Tunnels:
Total mobile ip tunnels 1
Tunnel0:
    src 10.1.1.11, dest 10.1.1.10 Key 6
    encap IP/IP, mode reverse-allowed, tunnel-users 1
    IP MTU 1480 bytes
    Path MTU Discovery, mtu: 0, ager: 10 mins, expires: never
    outbound interface Ethernet1/0
    MR created, fast switching enabled, ICMP unreachable enabled
    4 packets input, 306 bytes, 0 drops
    6 packets output, 436 bytes
    Template configuration:
        ip pim sparse-dense-mode
```

The below table describes the significant fields shown in the display.

Table 22: show ip mobile tunnel Field Descriptions

Field	Description
src	Tunnel source IP address.
dest	Tunnel destination IP address.
Key	Identifies the tunnel when there are multiple tunnels between the same end points (source address and destination address) for multipath support. This situation can occur if a mobile router registers through foreign agents on different interfaces. All of the HA-MR tunnels would have the same end points.
encap	Tunnel encapsulation type.
mode	Either reverse-allowed or reverse-off for reverse tunnel mode.
tunnel-users	Number of users on the tunnel.
HA created	Entity that created the tunnel. This field can be one of three values: HA created, FA created, or MR created.
fast switching	Enabled or disabled.
ICMP unreachable	Enabled or disabled.
packets input	Number of packets in.
bytes	Number of bytes in.
drops	Number of packets dropped. Packets are dropped when there are no visitors to send to after the foreign agent deencapsulates incoming packets. This prevents loops because the foreign agent will otherwise route the de-encapsulated packets back to the home agent.
packets output	Number of packets output.
bytes	Number of bytes output.
Route Map is	Name of the route map.

Field	Description
Running template configuration	If tunnel templates for multicast are enabled or disabled, this information is displayed or absent, respectively.

Related Commands

Command	Description
show ip mobile binding	Displays the mobility binding table.
show ip mobile host	Displays mobile node information.
show ip mobile visitor	Displays the table that contains a visitor list of foreign agents.

show ip mobile violation

To display information about security violations, use the **show ip mobile violation**command in privileged EXEC mode.

show ip mobile violation [*address*| **nai** *string*]

Syntax Description

address	(Optional) Displays violations from a specific IP address.
nai *string*	(Optional) Network access identifier.

Command Modes

EXEC

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2(2)XC	The nai keyword and associated parameters were added.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines

The most recent violation is saved for all the mobile nodes. A circular log holds up to 50 unknown requesters, which are the violators without security associations. The oldest violations will be purged to make room for new unknown requesters when the log limit is reached.

Security violation messages are logged at the informational level (see the **logging** global configuration command). When logging is enabled to include this severity level, violation history can be displayed using the **show logging** command.

Examples

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

```
Router# show ip mobile violation
Security Violation Log:

Mobile Hosts:
20.0.0.1:
    Violations: 1, Last time: 06/18/97 01:16:47
    SPI: 300, Identification: B751B581.77FD0E40
    Error Code: MN failed authentication (131), Reason: Bad authenticator (2)
```

The below table describes significant fields shown in the display.

Table 23: show ip mobile violation Field Descriptions

Field	Description
IP address	IP address of the violator. The network access identifier (NAI) is displayed if configured.
Violations	Total number of security violations for this peer.
Last time	Time of the most recent security violation for this peer.
SPI	SPI of the most recent security violation for this peer. If the security violation is due to an identification mismatch, then this is the SPI from the mobile-home authentication extension. If the security violation is due to an invalid authenticator, then this is the SPI from the offending authentication extension. In all other cases, it should be set to zero.
Identification	Identification used in request or reply of the most recent security violation for this peer.
Error Code	Error code in request or reply.
Reason Codes	Reason for the most recent security violation for this peer. Possible reasons are: • (1) No mobility security association • (2) Bad authenticator • (3) Bad identifier • (4) Bad SPI • (5) Missing security extension • (6) Other

show ip mobile visitor

To display the visitor table that contains information on mobile nodes (MNs) using this foreign agent (FA), use the **show ip mobile visitor**command inprivilegedEXEC mode.

show ip mobile visitor [[**pending**] [*ip-address*| **summary**]| **nai** *string* [**session-id** *string*]]

Syntax Description

pending	(Optional) Displays the pending registration table.
ip-address	(Optional) IP address of visiting MNs.
summary	(Optional) Displays all values in the table.
nai *string*	(Optional) Network access identifier (NAI).
session-id *string*	(Optional) Session identifier. The string value must be fewer than 25 characters.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2(2)XC	The nai keyword was added.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.3(4)T	The **session-id** keyword was added.
12.3(8)T	The output was enhanced to display UDP tunneling.

Usage Guidelines

Use this command to find out information on MNs that are registered with their (home agent) HA via this FA. The FA updates the visitor table that contain a list of the MNs using a FA.

A session identifier is used to uniquely identify a Mobile IP flow. A Mobile IP flow is the set of {NAI, IP address}. The flow allows a single NAI to be associated with one or multiple IP addresses, for example, {NAI, ipaddr1}, {NAI, ipaddr2}, and so on. A single user can have multiple sessions for example, when logging through different devices such as a PDA, cellular phone, or laptop. If the session identifier is present in the initial registration, it must be present in all subsequent registration renewals from that MN.

Examples

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

```
Router# show ip mobile visitor
Mobile Visitor List:
Total 1
10.0.0.1:
 Interface Ethernet1/2, MAC addr 0060.837b.95ec
 IP src 20.0.0.1, dest 67.0.0.31, UDP src port 434
 HA addr 66.0.0.5, Identification B7510E60.64436B38
 Lifetime 08:20:00 (30000) Remaining 08:19:16
 Tunnel100 src 68.0.0.31, dest 66.0.0.5, reverse-allowed
 Routing Options - (T)Reverse-tunnel
```

If the mobile node has visited and is associated with a session identifier, then the visitor entry for the mobile node shows the session identifier as shown below:

```
Router# show ip mobile visitor

Mobile Visitor List:
Total 1
 user01@cisco.com
 Home addr 100.100.100.17
  Interface Ethernet3/3, MAC addr 0004.6d25.b857
  IP src 0.0.0.0, dest 100.100.100.1, UDP src port 434
  HA addr 100.100.100.100, Identification BC189864.B2FE6CC4
  Lifetime 00:33:20 (2000) Remaining 00:33:06
  Tunnel0 src 70.70.70.2, dest 100.100.100.100, reverse-allowed
  Routing Options - (B)Broadcast
  Session identifier PD
```

The following sample output shows that the MN is registering with the HA (at the FA):

```
Router# show ip mobile visitor
Mobile Visitor List:
Total 1
10.99.100.2:
 Interface FastEthernet3/0, MAC addr 00ff.ff80.002b
 IP src 10.99.100.2, dest 30.5.3.5, UDP src port 434
 HA addr 200.1.1.1, Identification BCE7E391.A09E8720
 Lifetime 01:00:00 (3600) Remaining 00:30:09
 Tunnel1 src 200.1.1.5, dest 200.1.1.1, reverse-allowed
 Routing Options - (T)Reverse Tunneling
```

The below table describes the significant fields shown in the display.

Table 24: show ip mobile visitor Field Descriptions

Field	Description
Total	Number of mobile nodes visiting the foreign agent.
10.0.0.1	Home IP address of a visitor. The NAI is displayed if configured.
Interface	Interface the FA received the MN’s registration on.
MAC addr	MAC address of the visitor.
IP src	Source IP address of the registration request of a visitor.

Field	Description
IP dest	Destination IP address of the registration request of a visitor. A MN solicits an advertisement from the FA, and the FA uses the output interface's address (where it received the solicitation) as the source IP address in the advertisement. The MN picks up on this address and sends in a RRQ to it. This tells you which destination address the MN used when it sent in its registration request to the FA (typically the interface address). If it had sent the registration request to a broadcast or multicast address, or advertised address (not knowing the interface address), the FA will reply using the output interface address (typically the interface where it received the RRQ).
UDP src port	UDP src port used by the visiting mobile node in its registration request.
HA addr	Home agent IP address for that visiting mobile node.
Identification	Identification used in that registration by the mobile node.
Lifetime	The lifetime (in hh:mm:ss) granted to the mobile node for this registration.
Remaining	The time (in hh:mm:ss) remaining until the registration is expired. It has the same initial value as in the Lifetime field, and is counted down by the foreign agent.
Tunnel	The tunnel used by the mobile node is characterized by the source and destination addresses, and reverse-allowed or reverse-off for reverse tunnel. The options are IPIP, GRE, and UDP. The default is IPIP encapsulation.

Field	Description
Routing Options	Routing options list all foreign agent-accepted services, based on registration flags sent by the mobile node. Options are: • (S) Multi-binding (not supported on home agent) • (B) Broadcast • (D) Direct-to-mobile node • (M) MinIP (not supported on home agent) • (G) GRE • (T) Reverse-tunnel
Session identifier	Session identifier can be the device name or MAC address.

Related Commands

Command	Description
debug ip mobile	Displays IP mobility activities.
ip mobile foreign-agent nat traversal	Enables NAT UDP traversal support for MIP FAs.
ip mobile home-agent nat traversal	Enables NAT UDP traversal support for MIP HAs.
show ip mobile binding	Displays the mobility binding table.
show ip mobile globals	Displays global information about MIP HAs, FAs, and MNs.
show ip mobile tunnel	Displays information about UDP tunneling.

show ip mobile vpn-realm

To display virtual private network (VPN) realms configured for Mobile IP, use the **show ip mobile vpn-realm**command in EXEC mode.

show ip mobile vpn-realm

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

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

Usage Guidelines

Use this command to display VPN realms configured by the **ip mobile vpn-realm**command**.**

Examples

The following example output shows which VPN realms and corresponding sequence numbers are configured for Mobile IP:

```
Router# show ip mobile vpn-realm
IP Mobile VPN realm(s):
    Sequence number: 20      Realm: company1
    Sequence number: 10      Realm: company2
```

Related Commands

Command	Description
ip mobile vpn-realm	Defines VPN realms to be used in home agent policy routing.

show ipv6 mobile pmipv6 lma binding

To display the list of the Local Mobility Anchor (LMA) bindings established over the Proxy Mobile IPv6 (PMIPv6) signaling plane, use the **show ipv6 mobile pmipv6 lma binding** command in privileged EXEC mode.

show ipv6 mobile pmipv6 lma binding [**mag** *peer-id* | **nai** *string*]

Syntax Description

mag *peer-id*	(Optional) Displays the bindings for the Mobile Access Gateway (MAG).
nai *string*	(Optional) Displays the bindings for the mobile node (MN).

Command Default

The list of the bindings established over the Proxy Mobile IPv6 (PMIPv6) signaling plane is displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.6S	This command was introduced.
15.2(4)M	This command was integrated into Cisco IOS Release 15.2(4)M.
Cisco IOS XE Release 3.9S	This command was modified. The command output was enhanced to display the third-generation mobility anchor (3GMA) bindings.

Examples

The following is sample output from the **show ipv6 mobile pmipv6 mag binding** command. The fields in the display are self-explanatory.

```
Device# show ipv6 mobile pmipv6 lma binding

Total number of bindings: 1
----------------------------------------
[Binding][MN]: Domain: D1, NAI: MN1@example.com
[Binding][MN]: HOA: 16.16.16.2, Prefix: 24
[Binding][MN]: HNP: 0
[Binding][MN][PEER]: Default Router: 16.16.16.1
        [Binding][MN]: ATT: 3GPP_GERAN (6)
                 [Binding][MN][PEER1]:LLID: aabb.cc01.2d00:MN1@c3GMA
                 [Binding][MN][PEER1]: Id: 3GMA
                 [Binding][MN][PEER1]: Lifetime: 10(sec)
                 [Binding][MN][PEER1]: Lifetime Remaining: 5(sec)
        [Binding][MN]: ATT: WLAN (4)
                 [Binding][MN][PEER2]:LLID: aabb.cc01.2d00
                 [Binding][MN][PEER2]: Id: WIFI_MAG
```

```
                [Binding][MN][PEER2]: Lifetime: 10(sec)
                [Binding][MN][PEER2]: Lifetime Remaining: 8(sec)
                [Binding][MN][PEER2]: Tunnel: Tunnel0
                [Binding][MN][GREKEY]: Upstream: 10, Downstream: 10
```

The table below describes the significant fields shown in the display.

Table 25: show ipv6 mobile pmipv6 lma binding Field Descriptions

Field	Description
Domain	Configured PMIPV6 domain.
HOA	Home address.
HNP	Home network prefix.
Default Router	IP address of the default router.
LLID	Link layer identifier.
Id	Peer identifier.
Lifetime	Total lifetime (in hh:mm:ss) of the 3GPP binding cache entry (BCE).
Lifetime Remaining	The time (in hh:mm:ss) remaining until the binding expires.
Tunnel	The tunnel used by the mobile node is characterized by the source and destination addresses and reverse-allowed or reverse-off for reverse tunnel.
Upstream	Upstream Generic Routing Encapsulation (GRE) Key.
Downstream	Downstream GRE Key.

The following is sample output from the **show ipv6 mobile pmipv6 lma binding mag** *peer-id* command. The fields in the display are self-explanatory.

```
Device# show ipv6 mobile pmipv6 lma binding mag lma1

Total number of bindings: 1
----------------------------------------
[Binding][MN]: Domain: D1, Nai: example1@example.com
        [Binding][MN]: State: ACTIVE
        [Binding][MN]: Interface: GigabitEthernet0/0/0
        [Binding][MN]: Hoa: 0x11110002, att: 3, llid: aabb.cc00.c900
        [Binding][MN][LMA]: Id: LMA1
        [Binding][MN][LMA]: lifetime: 3600
```

Related Commands

Command	Description
ipv6 mobile pmipv6-lma	Configures the LMA for the PMIP domain.

show ipv6 mobile pmipv6 lma globals

To display the Local Mobility Anchor (LMA) global configuration details, use the **show ipv6 mobile pmipv6 lma globals** command in privileged EXEC mode.

show ipv6 mobile pmipv6 lma globals

Syntax Description

This command has no arguments or keywords.

Command Default

The contents of the LMA configuration file, except for the default configuration.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.6S	This command was introduced.
15.2(4)M	This command was integrated into Cisco IOS Release 15.2(4)M.

Examples

The following is sample output from the **show ipv6 mobile pmipv6 lma globals** command. The fields in the display are self-explanatory.

```
Device# show ipv6 mobile pmipv6 lma globals

Domain  : D1

LMA Identifier  : lma1
        AAA Accounting                  : Disabled
        Default MN Profile              : profile1
        Network                         : n1
        IPv4 Pool Name                  : v4 Prefix Length: 24
        IPv6 Pool Name                  : v6pool Prefix Length: 48
        Max. HNPs                       : 1
        Max Bindings                    : 128000
        AuthOption                      : disabled
        RegistrationLifeTime            : 3600 (sec)
        DeleteTime                      : 10000 (msec)
        CreateTime                      : 1500 (msec)
        BRI InitDelayTime               : 1000 (msec)
        BRI MaxDelayTime                : 2000 (msec)
        BRI MaxRetries                  : 1
        BRI EncapType                   : IPV6_IN_IPV6
        Fixed Link address is           : enabled
        Fixed Link address              : 6161.6262.2e63
        Fixed Link Local address is     : enabled
        Fixed Link local address        : FE80::8
        RefreshTime                     : 300 (sec)
        Refresh RetxInit time           : 1000 (msec)
        Refresh RetxMax time            : 32000 (msec)
        Timestamp option                : enabled
        Validity Window                 : 10
```

```
Peer :  mag1
        Max. HNPs                       : 1
        Max Bindings                    : 128000
        AuthOption                      : disabled
        RegistrationLifeTime            : 3600 (sec)
        DeleteTime                      : 10000 (msec)
        CreateTime                      : 1500 (msec)
        BRI InitDelayTime               : 1000 (msec)
        BRI MaxDelayTime                : 2000 (msec)
        BRI MaxRetries                  : 1
        BRI EncapType                   : IPV6_IN_IPV6
        Fixed Link address is           : enabled
        Fixed Link address              : 6161.6262.2e63
        Fixed Link Local address is     : enabled
        Fixed Link local address        : FE80::8
        RefreshTime                     : 300 (sec)
        Refresh RetxInit time           : 1000 (msec)
        Refresh RetxMax time            : 32000 (msec)
        Timestamp option                : enabled
        Validity Window                 : 10

Peer :  mag0
        Max. HNPs                       : 1
        Max Bindings                    : 128000
        AuthOption                      : disabled
        RegistrationLifeTime            : 3600 (sec)
        DeleteTime                      : 10000 (msec)
        CreateTime                      : 1500 (msec)
        BRI InitDelayTime               : 1000 (msec)
        BRI MaxDelayTime                : 2000 (msec)
        BRI MaxRetries                  : 1
        BRI EncapType                   : GRE in IPV4
        Fixed Link address is           : enabled
        Fixed Link address              : 6161.6262.2e63
        Fixed Link Local address is     : enabled
        Fixed Link local address        : FE80::8
        RefreshTime                     : 300 (sec)
        Refresh RetxInit time           : 1000 (msec)
        Refresh RetxMax time            : 32000 (msec)
        Timestamp option                : enabled
        Validity Window                 : 10
```

Related Commands

Command	Description
ipv6 mobile pmipv6-lma	Configures the LMA for the PMIP domain.

show ipv6 mobile pmipv6 lma stats

To display the global Local Mobility Anchor (LMA) statistics, use the **show ipv6 mobile pmipv6 lma stats** command in privileged EXEC mode.

show ipv6 mobile pmipv6 lma stats [**domain** *domain-name* **peer** *peer-name*]

Syntax Description

domain *domain-name*	(Optional) Specifies the Proxy Mobile IPv6 (PMIPv6) domain.
peer *peer-name*	(Optional) Specifies the Mobile Access Gateway (MAG).

Command Modes

Privileged EXEC (#)

Command History

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

Examples

The following is sample output from the **show ipv6 mobile pmipv6 lma stats** command:

```
Router# show ipv6 mobile pmipv6 lma stats

----------------------------------------
[lma1] Stats: Total Bindings:1
Proxy Binding Update Received Stats
Total                         : 2260    Drop                          : 0
AAA Accounting Stats
Start Accounting Sent         : 0       Stop Accounting Sent          : 0
-------------------------------------------------
Proxy Binding Acknowledgment Sent Stats
Total                         : 2260    Drop                          : 0
BA_ACCEPTED                   : 2259    BA_UNKNOWN                    : 0
BA_UNSPEC_FAIL                : 0       BA_ADMIN_FAIL                 : 0
BA_RESOURCE_FAIL              : 0       BA_HM_REG_FAIL                : 0
BA_HM_SUBNET_FAIL             : 0       BA_BAD_SEQ_FAIL               : 0
BA_CHANGE_FAIL                : 0       BA_AUTH_FAIL                  : 0
PROXY_REG_NOT_ENABLED         : 0       NOT_LMA_FOR_THIS_MN           : 0
MAG_NOT_AUTH_FOR_PROXY_REG    : 0       NOT_AUTHORIZED_FOR_HNP        : 0
TIMESTAMP_MISMATCH            : 0       TIMESTAMP_LOWER_THAN_PREV     : 1
MISSING_HNP_OPTION            : 0       BCE_PBU_PFX_SET_DO_NOT_MATCH  : 0
MISSING_MN_IDENTIFIER_OPTION  : 0       MISSING_HI_OPTION             : 0
NOT_AUTH_FOR_IPV4_MOBILITY    : 0       NOT_AUTH_FOR_IPV4_HOME_ADDRESS: 0
NOT_AUTH_FOR_IPV6_MOBILITY    : 0       MULTIPLE_IPV4_HOA_NO_SUPPORT  : 0
GRE_KEY_OPTION_NOT_REQUIRED   : 0
-------------------------------------------------
Proxy Binding Revocation Acknowledgment Received Stats
Total                         : 0       Drop                          : 0
BR_SUCCESS                    : 0       BR_PARTIAL_SUCCESS            : 0
BR_NO_BINDING                 : 0       BR_HOA_REQUIRED               : 0
BR_GLOBAL_REVOC_NOT_AUTH      : 0       BR_MN_IDENTITY_REQUIRED       : 0
```

```
BR_MN_ATTACHED                : 0       BR_UNKNOWN_REVOC_TRIGGER      : 0
BR_REVOC_FUNC_NOT_SUPPORTED   : 0       BR_PBR_NOT_SUPPORTED_STATS    : 0
-------------------------------------------------
Proxy Binding Revocation Acknowledgment Sent Stats
Total                         : 0       Drop                          : 0
BR_SUCCESS                    : 0       BR_PARTIAL_SUCCESS            : 0
BR_NO_BINDING                 : 0       BR_HOA_REQUIRED               : 0
BR_GLOBAL_REVOC_NOT_AUTH      : 0       BR_MN_IDENTITY_REQUIRED       : 0
BR_MN_ATTACHED                : 0       BR_UNKNOWN_REVOC_TRIGGER      : 0
BR_REVOC_FUNC_NOT_SUPPORTED   : 0       BR_PBR_NOT_SUPPORTED_STATS    : 0
-------------------------------------------------
Proxy Binding Revocation Indication Received Stats
Total                         : 0       Drop                          : 0
BR_UNSPECIFIED                : 0       BR_ADMIN_REASON               : 0
BR_MAG_HANDOVER_SAME_ATT      : 0       BR_MAG_HANDOVER_DIFF_ATT      : 0
BR_MAG_HANDOVER_UNKNOWN       : 0       BR_USER_SESS_TERMINATION      : 0
BR_NETWORK_SESS_TERMINATION   : 0       BR_OUT_OF_SYNC_BCE_STATE      : 0
BR_PER_PEER_POLICY            : 0       BR_REVOKING_MN_LOCAL_POLICY   : 0
-------------------------------------------------
Proxy Binding Revocation Indication Sent Stats
Total                         : 0       Drop                          : 0
BR_UNSPECIFIED                : 0       BR_ADMIN_REASON               : 0
BR_MAG_HANDOVER_SAME_ATT      : 0       BR_MAG_HANDOVER_DIFF_ATT      : 0
BR_MAG_HANDOVER_UNKNOWN       : 0       BR_USER_SESS_TERMINATION      : 0
BR_NETWORK_SESS_TERMINATION   : 0       BR_OUT_OF_SYNC_BCE_STATE      : 0
BR_PER_PEER_POLICY            : 0       BR_REVOKING_MN_LOCAL_POLICY   : 0

-------------------------------------------------
MM Stats
Drop                          : 0       Checksum Error                : 0
```

The table below describes the significant fields shown in the display. The other fields are self-explanatory.

Table 26: show ipv6 mobile pmipv6 mag stats Field Descriptions

Field	Description
Proxy Binding Update Received Stats	The Proxy Binding Update (PBU) received by the LMA.
Proxy Binding Acknowledgment Sent Stats	The Proxy Binding Revocation Acknowledgment (PBRA) message sent from the LMA to the MAG and vice versa.
Proxy Binding Revocation Acknowledgment Received Stats	The Proxy Binding Revocation Acknowledgment (PBRA) message received by the MAG from the LMA and vice versa.
Proxy Binding Revocation Acknowledgment Sent Stats	The Proxy Binding Revocation Acknowledgment (PBRA) message sent from from the LMA to the MAG and vice versa.
Proxy Binding Revocation Indication Received Stats	The Proxy Binding Revocation Indication (PBRI) message received by the MAG from the LMA and vice versa.
Proxy Binding Revocation Indication Sent Stats	The Proxy Binding Revocation Indication message sent from the LMA to the MAG and vice versa.

The following is sample output from the **show ipv6 mobile pmipv6 lma stats domain** command:

```
Device# show ipv6 mobile pmipv6 lma stats domain D1 peer MAG1
----------------------------------------
[MAG1]: PBU Sent                : 7
[MAG1]: PBA Rcvd                : 6
[MAG1]: PBRI Sent               : 0
[MAG1]: PBRI Rcvd               : 0
[MAG1]: PBRA Sent               : 0
[MAG1]: PBRA Rcvd               : 0
[MAG1]: No Of handoff   : 0
```

Related Commands

Command	Description
ipv6 mobile pmipv6-mag	Configures the MAG for the PMIP domain.
show interfaces tunnel 0 stats	Displays the PMIP tunnel statistics.

show ipv6 mobile pmipv6 lma tunnel

To display details of the Local Mobility Anchor (LMA) tunnels, use the **show ipv6 mobile pmipv6 lma tunnel** command in privileged EXEC mode.

show ipv6 mobile pmipv6 lma tunnel

Syntax Description

This command has no arguments or keywords.

Command Default

The details of the LMA tunnels are displayed.

Command Modes

Privileged EXEC (#)

Command History

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

Examples

The following is sample output from the **show ipv6 mobile pmipv6 lma tunnel** command:

```
Router# show ipv6 mobile pmipv6 lma tunnel

[lma1] Tunnel Information
Peer [mag0] : Tunnel Bindings 1
  Tunnel0:
        src 10.10.10.2, dest 172.16.0.0
        encap GRE/IP, mode reverse-allowed
        key 0, Outbound Interface Ethernet0/0
    6 packets input, 600 bytes, 0 drops
    6 packets output, 600 bytes
```

Related Commands

Command	Description
ipv6 mobile pmipv6-lma	Configures the LMA for the PMIPv6 domain.

show ipv6 mobile pmipv6 mag binding

To display the list of the Mobile Access Gateway (MAG) bindings established over the Proxy Mobile IPv6 (PMIPv6) signaling plane, use the **show ipv6 mobile pmipv6 mag binding** command in privileged EXEC mode.

Cisco IOS XE Release 3.4S

show ipv6 mobile pmipv6 mag binding [**lma** *lma-id*| **nai** *string*]

Cisco IOS XE Release 3.6S

show ipv6 mobile pmipv6 mag binding [**lma**| **nai** *string*]

Cisco IOS Release 15.2(4)M and Later Releases

show ipv6 mobile pmipv6 mag *mag-id* **binding** [**lma**| **nai** *string*]

Syntax Description

mag-id	MAG identifier.
lma	(Optional) Displays the bindings for the Local Mobility Anchor (LMA).
lma-id	(Optional) LMA identifier.
nai *string*	(Optional) Displays the bindings for the mobile node (MN).

Command Default

The MAG bindings established over the PMIPv6 signaling plane are displayed.

Command Modes

Privileged EXEC (#)

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 *lma-identifier* argument was removed.
15.2(4)M	This command was modified. This command was integrated into Cisco IOS Release 15.2(4)M. The *mag-id* argument was added.

Usage Guidelines

In the Cisco IOS XE Release 3.4S, the **lma** *lma-identifier* keyword-argument pair is available.

Examples

The following is sample output from the **show ipv6 mobile pmipv6 mag binding** command. The fields in the display are self-explanatory.

```
Device# show ipv6 mobile pmipv6 mag mag1 binding

Total number of bindings: 2
----------------------------------------
[Binding][MN]: Domain: D1, Nai: MN1@example.com
        [Binding][MN]: State: ACTIVE
        [Binding][MN]: Interface: GigabitEthernet0/1/0
        [Binding][MN]: Hoa: 0x11110002, att: 3, llid: aabb.cc00.c900
        [Binding][MN][LMA]: Id: LMA1
        [Binding][MN][LMA]: lifetime: 3600
----------------------------------------
----------------------------------------
[Binding][MN]: Domain: D1, Nai: MN3@example.com
        [Binding][MN]: State: ACTIVE
        [Binding][MN]: Interface: GigabitEthernet0/0/0
        [Binding][MN]: Hoa: 0x11110102, att: 3, llid: aabb.cc00.ce00
        [Binding][MN][LMA]: Id: LMA2
        [Binding][MN][LMA]: lifetime: 3600
----------------------------------------
```

The following is sample output from the **show ipv6 mobile pmipv6 mag binding lma** command. The fields in the display are self-explanatory.

```
Device# show ipv6 mobile pmipv6 mag mag1 binding lma

Total number of bindings: 1
----------------------------------------
[Binding][MN]: Domain: D1, Nai: MN1@example.com
        [Binding][MN]: State: ACTIVE
        [Binding][MN]: Interface: GigabitEthernet0/0/0
        [Binding][MN]: Hoa: 0x11110002, att: 3, llid: aabb.cc00.c900
        [Binding][MN][LMA]: Id: LMA1
        [Binding][MN][LMA]: lifetime: 3600
----------------------------------------
```

Related Commands

Command	Description
ipv6 mobile pmipv6-mag	Configures the MAG for the PMIPv6 domain.

show ipv6 mobile pmipv6 mag globals

To display the Mobile Access Gateway (MAG) global configuration details, use the **show ipv6 mobile pmipv6 mag globals** command in privileged EXEC mode.

show ipv6 mobile pmipv6 mag *mag-id* **globals**

Syntax Description

mag-id	MAG identifier.

Command Default

The **show ipv6 mobile pmipv6 mag globals** command displays contents of the MAG configuration file, except for the default configuration.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

The **show ipv6 mobile pmipv6 mag globals** command displays the configuration settings related to the MAG service.

Examples

The following is sample output from the **show ipv6 mobile pmipv6 mag globals** command. The fields in the display are self-explanatory.

```
Router# show ipv6 mobile pmipv6 mag mag1 globals
Domain  : D1
Mag Identifier  : M1
        MN's detach discover            : disabled
        Local routing                   : disabled
        Mag is enabled on interface     : GigabitEthernet0/0/0
        Mag is enabled on interface     : GigabitEthernet0/1/0
        Max Bindings                    : 3
        AuthOption                      : disabled
        RegistrationLifeTime            : 3600 (sec)
        BRI InitDelayTime               : 1000 (msec)
        BRI MaxDelayTime                : 40000 (msec)
        BRI MaxRetries                  : 6
        BRI EncapType                   : IPV6_IN_IPV6
        Fixed Link address is           : enabled
        Fixed Link address              : aaaa.aaaa.aaaa
        Fixed Link Local address is     : enabled
        Fixed Link local address        : 0xFE800000 0x0 0x0 0x2
        RefreshTime                     : 300 (sec)
        Refresh RetxInit time           : 20000 (msec)
        Refresh RetxMax time            : 50000 (msec)
        Timestamp option                : enabled
        Validity Window                 : 7
          !
Peer :  LMA1
        Max Bindings                    : 3
        AuthOption                      : disabled
        RegistrationLifeTime            : 3600 (sec)
        BRI InitDelayTime               : 1000 (msec)
        BRI MaxDelayTime                : 40000 (msec)
        BRI MaxRetries                  : 6
        BRI EncapType                   : IPV6_IN_IPV6
        Fixed Link address is           : enabled
        Fixed Link address              : aaaa.aaaa.aaaa
        Fixed Link Local address is     : enabled
        Fixed Link local address        : 0xFE800000 0x0 0x0 0x2
        RefreshTime                     : 300 (sec)
        Refresh RetxInit time           : 20000 (msec)
        Refresh RetxMax time            : 50000 (msec)
        Timestamp option                : enabled
        Validity Window                 : 7
!
Peer :  LMA2
        Max Bindings                    : 3
        AuthOption                      : disabled
        RegistrationLifeTime            : 3600 (sec)
        BRI InitDelayTime               : 1000 (msec)
        BRI MaxDelayTime                : 40000 (msec)
        BRI MaxRetries                  : 6
        BRI EncapType                   : IPV6_IN_IPV6
        Fixed Link address is           : enabled
        Fixed Link address              : aaaa.aaaa.aaaa
        Fixed Link Local address is     : enabled
        Fixed Link local address        : 0xFE800000 0x0 0x0 0x2
        RefreshTime                     : 300 (sec)
        Refresh RetxInit time           : 20000 (msec)
        Refresh RetxMax time            : 50000 (msec)
        Timestamp option                : enabled
        Validity Window                 : 7
```

Related Commands

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

show ipv6 mobile pmipv6 mag stats

To display global Mobile Access Gateway (MAG) statistics, use the **show ipv6 mobile pmipv6 mag stats** command in privileged EXEC mode.

show ipv6 mobile pmipv6 mag *mag-id* **stats** [**domain** *domain-name* **peer** *peer-name*]

Syntax Description

mag-id	MAG identifier.
domain *domain-name*	(Optional) Specifies the Proxy Mobile IPv6 (PMIPV6) domain.
peer *peer-name*	(Optional) Specifies the Local Mobility Anchor (LMA).

Command Default

The **show ipv6 mobile pmipv6 mag stats** command displays MAG statistics.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

The **show ipv6 mobile pmipv6 mag stats domain** *domain-name* **peer** *peer-name* command displays statistics related to the LMA.

Examples

The following is sample output from the **show ipv6 mobile pmipv6 mag stats** command:

```
Device# show ipv6 mobile pmipv6 mag mag1 stats

----------------------------------------
[M1]: Total Bindings     : 2
[M1]: PBU Sent           : 14
[M1]: PBA Rcvd           : 7
[M1]: PBRI Sent          : 0
[M1]: PBRI Rcvd          : 0
[M1]: PBRA Sent          : 0
[M1]: PBRA Rcvd          : 0
[M1]: No Of handoff      : 0
```

The below table describes the significant fields shown in the display. The remaining fields are self-explanatory.

Table 27: show ipv6 mobile pmipv6 mag stats Field Descriptions

Field	Description
PBU Sent	The Proxy Binding Update (PBU) that is sent from the MAG to the LMA.
PBA Rcvd	The Proxy Binding Acknowledgment (PBA) that is received by the MAG.
PBRI Sent	The Proxy Binding Revocation Indication (PBRI) message that is sent from the LMA to the MAG and vice versa.
PBRI Rcvd	The PBRI message that is received by the LMA from the MAG and vice versa.
PBRA Sent	The Proxy Binding Revocation Acknowledgment (PBRA) message that is sent from the MAG to the LMA and vice versa.
PBRA Rcvd	The PBRA message that is received by the MAG from the LMA and vice versa.
No Of handoff	The number of the handoffs between different interfaces of the MAG.

The following is sample output from the **show ipv6 mobile pmipv6 mag stats domain** *domain-name* **peer** *peer-name* command:

```
Router# show ipv6 mobile pmipv6 mag mag1 stats domain D1 peer LMA1
----------------------------------------
[LMA1]: PBU Sent                : 7
[LMA1]: PBA Rcvd                : 6
[LMA1]: PBRI Sent               : 0
[LMA1]: PBRI Rcvd               : 0
[LMA1]: PBRA Sent               : 0
[LMA1]: PBRA Rcvd               : 0
[LMA1]: No Of handoff   : 0
```

Related Commands

Command	Description
ipv6 mobile pmipv6-mag	Configures the MAG for the PMIPV6 domain.
show interfaces tunnel 0 stats	Displays the PMIPV6 tunnel statistics.

show ipv6 ospf

To display general information about Open Shortest Path First (OSPF) routing processes, use the **show ipv6 ospf** command in user EXEC or privileged EXEC mode.

show ipv6 ospf [*process-id*] [*area-id*] **[rate-limit]**

Syntax Description

process-id	(Optional) Internal identification. It is locally assigned and can be any positive integer. The number used here is the number assigned administratively when the OSPF routing process is enabled.
area-id	(Optional) Area ID. This argument displays information about a specified area only.
rate-limit	(Optional) Rate-limited link-state advertisements (LSAs). This keyword displays LSAs that are currently being rate limited, together with the remaining time to the next generation.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.3(4)T	Command output is changed when authentication is enabled.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(9)T	Command output was updated to display OSPF for IPv6 encryption information.
12.4(15)XF	Command output was modified to include VMI PPPoE process-level values.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T

Release	Modification
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SRC	The **rate-limit** keyword was added. Command output was modified to include the configuration values for SPF and LSA throttling timers.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
15.0(1)M	This command was integrated into Cisco IOS Release 12.5(1)M.
15.1(2)T	This command was modified. Support for IPv6 was added to Cisco IOS Release 15.1(2)T.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.
15.1(1)SG	This command was integrated into Cisco IOS Release 15.1(1)SG.
15.0(1)SY	This command was integrated into Cisco IOS Release 15.0(1)SY.
15.2(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services devices.

Examples

Examples

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

```
Device# show ipv6 ospf
Routing Process "ospfv3 1" with ID 10.10.10.1
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
 LSA group pacing timer 240 secs
 Interface flood pacing timer 33 msecs
 Retransmission pacing timer 66 msecs
 Number of external LSA 0. Checksum Sum 0x000000
 Number of areas in this device is 1. 1 normal 0 stub 0 nssa
    Area BACKBONE(0)
        Number of interfaces in this area is 1
        MD5 Authentication, SPI 1000
        SPF algorithm executed 2 times
        Number of LSA 5. Checksum Sum 0x02A005
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0
```

The table below describes the significant fields shown in the display.

Table 28: show ipv6 ospf Field Descriptions

Field	Description
Routing process "ospfv3 1" with ID 10.10.10.1	Process ID and OSPF device ID.

Field	Description
LSA group pacing timer	Configured LSA group pacing timer (in seconds).
Interface flood pacing timer	Configured LSA flood pacing timer (in milliseconds).
Retransmission pacing timer	Configured LSA retransmission pacing timer (in milliseconds).
Number of areas	Number of areas in device, area addresses, and so on.

Examples

The following sample output shows the **show ipv6 ospf** command with area encryption information:

```
Device# show ipv6 ospf
Routing Process "ospfv3 1" with ID 10.0.0.1
It is an area border device
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
LSA group pacing timer 240 secs
Interface flood pacing timer 33 msecs
Retransmission pacing timer 66 msecs
Number of external LSA 0. Checksum Sum 0x000000
Number of areas in this device is 2. 2 normal 0 stub 0 nssa
Reference bandwidth unit is 100 mbps
    Area BACKBONE(0)
        Number of interfaces in this area is 2
        SPF algorithm executed 3 times
        Number of LSA 31. Checksum Sum 0x107493
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 20
        Flood list length 0
    Area 1
        Number of interfaces in this area is 2
        NULL Encryption SHA-1 Auth, SPI 1001
        SPF algorithm executed 7 times
        Number of LSA 20. Checksum Sum 0x095E6A
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0
```

The table below describes the significant fields shown in the display.

Table 29: show ipv6 ospf with Area Encryption Information Field Descriptions

Field	Description
Area 1	Subsequent fields describe area 1.
NULL Encryption SHA-1 Auth, SPI 1001	Displays the encryption algorithm (in this case, null, meaning no encryption algorithm is used), the authentication algorithm (SHA-1), and the security policy index (SPI) value (1001).

The following example displays the configuration values for SPF and LSA throttling timers:

```
Device# show ipv6 ospf
 Routing Process "ospfv3 1" with ID 10.9.4.1
 Event-log enabled, Maximum number of events: 1000, Mode: cyclic
 It is an autonomous system boundary device
 Redistributing External Routes from,
    ospf 2
 Initial SPF schedule delay 5000 msecs
 Minimum hold time between two consecutive SPFs 10000 msecs
 Maximum wait time between two consecutive SPFs 10000 msecs
 Minimum LSA interval 5 secs
 Minimum LSA arrival 1000 msecs
```

The table below describes the significant fields shown in the display.

Table 30: show ipv6 ospf with SPF and LSA Throttling Timer Field Descriptions

Field	Description
Initial SPF schedule delay	Delay time of SPF calculations.
Minimum hold time between two consecutive SPFs	Minimum hold time between consecutive SPF calculations.
Maximum wait time between two consecutive SPFs 10000 msecs	Maximum hold time between consecutive SPF calculations.
Minimum LSA interval 5 secs	Minimum time interval (in seconds) between link-state advertisements.
Minimum LSA arrival 1000 msecs	Maximum arrival time (in milliseconds) of link-state advertisements.

The following example shows information about LSAs that are currently being rate limited:

```
Device# show ipv6 ospf rate-limit
List of LSAs that are in rate limit Queue
    LSAID: 0.0.0.0 Type: 0x2001 Adv Rtr: 10.55.55.55 Due in: 00:00:00.500
    LSAID: 0.0.0.0 Type: 0x2009 Adv Rtr: 10.55.55.55 Due in: 00:00:00.500
```

The table below describes the significant fields shown in the display.

Table 31: show ipv6 ospf rate-limit Field Descriptions

Field	Description
LSAID	Link-state ID of the LSA.
Type	Description of the LSA.
Adv Rtr	ID of the advertising device.
Due in:	Remaining time until the generation of the next event.

show ipv6 ospf interface

To display Open Shortest Path First (OSPF)-related interface information, use the **showipv6ospfinterface** command in user EXEC or privileged mode.

show ipv6 ospf [*process-id*] [*area-id*] **interface** [*type number*] **[brief]**

Syntax Description

process-id	(Optional) Internal identification. It is locally assigned and can be any positive integer. The number used here is the number assigned administratively when the OSPF routing process is enabled.
area-id	(Optional) Displays information about a specified area only.
type number	(Optional) Interface type and number.
brief	(Optional) Displays brief overview information for OSPF interfaces, states, addresses and masks, and areas on the router.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.3(4)T	Command output is changed when authentication is enabled.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(9)T	Command output is changed when encryption is enabled.
12.2(33)SRB	The **brief** keyword was added.

Release	Modification
12.4(15)XF	Output displays were modified so that VMI PPPoE interface-based local state values are displayed in the command output when a VMI interface is specified.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	Command output was updated to display graceful restart information.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.
15.1(1)SY	This command was was modified. It was integrated into Cisco IOS Release 15.1(1)SY.

Examples

Examples

The following is sample output from the **showipv6ospfinterface** command:

```
Router# show ipv6 ospf interface
ATM3/0 is up, line protocol is up
  Link Local Address 2001:0DB1:205:5FFF:FED3:5808, Interface ID 13
  Area 1, Process ID 1, Instance ID 0, Router ID 172.16.3.3
  Network Type POINT_TO_POINT, Cost: 1
  Transmit Delay is 1 sec, State POINT_TO_POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:06
  Index 1/2/2, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 12, maximum is 12
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 172.16.4.4
  Suppress hello for 0 neighbor(s)
FastEthernet0/0 is up, line protocol is up
  Link Local Address 2001:0DB1:205:5FFF:FED3:5808, Interface ID 3
  Area 1, Process ID 1, Instance ID 0, Router ID 172.16.3.3
  Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router (ID) 172.16.6.6, local address 2001:0DB1:205:5FFF:FED3:6408
  Backup Designated router (ID) 172.16.3.3, local address 2001:0DB1:205:5FFF:FED3:5808
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:05
  Index 1/1/1, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 12, maximum is 12
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 172.16.6.6  (Designated Router)
  Suppress hello for 0 neighbor(s)
```

The table below describes the significant fields shown in the display.

Table 32: show ipv6 ospf interface Field Descriptions

Field	Description
ATM3/0	Status of the physical link and operational status of protocol.
Link Local Address	Interface IPv6 address.
Area 1, Process ID 1, Instance ID 0, Router ID 172.16.3.3	The area ID, process ID, instance ID, and router ID of the area from which this route is learned.
Network Type POINT_TO_POINT, Cost: 1	Network type and link-state cost.
Transmit Delay	Transmit delay, interface state, and router priority.
Designated Router	Designated router ID and respective interface IP address.
Backup Designated router	Backup designated router ID and respective interface IP address.
Timer intervals configured	Configuration of timer intervals.
Hello	Number of seconds until the next hello packet is sent out this interface.
Neighbor Count	Count of network neighbors and list of adjacent neighbors.

Examples

The following is sample output of the **showipv6ospfinterface** command when the **brief** keyword is entered.

```
Router# show ipv6 ospf interface brief

Interface    PID   Area            Intf ID    Cost  State Nbrs F/C
VL0          6     0               21         65535 DOWN  0/0
Se3/0        6     0               14         64    P2P   0/0
Lo1          6     0               20         1     LOOP  0/0
Se2/0        6     6               10         62    P2P   0/0
Tu0          1000  0               19         11111 DOWN  0/0
```

Examples

The following is sample output from the **showipv6ospfinterface** command with authentication enabled on the interface:

```
Router# show ipv6 ospf interface
Ethernet0/0 is up, line protocol is up
  Link Local Address 2001:0DB1:A8BB:CCFF:FE00:6E00, Interface ID 2
  Area 0, Process ID 1, Instance ID 0, Router ID 10.10.10.1
  Network Type BROADCAST, Cost:10
  MD5 Authentication SPI 500, secure socket state UP (errors:0)
  Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router (ID) 10.11.11.1, local address 2001:0DB1:A8BB:CCFF:FE00:6F00
  Backup Designated router (ID) 10.10.10.1, local address
2001:0DB1:A8BB:CCFF:FE00:6E00
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:01
  Index 1/1/1, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 10.11.11.1  (Designated Router)
  Suppress hello for 0 neighbor(s)
```

Examples

The following is sample output from the **showipv6ospfinterface** command with null authentication configured on the interface:

```
Router# show ipv6 ospf interface
Ethernet0/0 is up, line protocol is up
  Link Local Address 2001:0DB1:A8BB:CCFF:FE00:6E00, Interface ID 2
  Area 0, Process ID 1, Instance ID 0, Router ID 10.10.10.1
  Network Type BROADCAST, Cost:10
  Authentication NULL
  Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router (ID) 10.11.11.1, local address 2001:0DB1:A8BB:CCFF:FE00:6F00
  Backup Designated router (ID) 10.10.10.1, local address
2001:0DB1:A8BB:CCFF:FE00:6E00
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:03
  Index 1/1/1, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 10.11.11.1  (Designated Router)
  Suppress hello for 0 neighbor(s)
```

Examples

The following is sample output from the **showipv6ospfinterface** command with authentication configured for the area:

```
Router# show ipv6 ospf interface
Ethernet0/0 is up, line protocol is up
  Link Local Address 2001:0DB1:A8BB:CCFF:FE00:6E00, Interface ID 2
  Area 0, Process ID 1, Instance ID 0, Router ID 10.10.10.1
  Network Type BROADCAST, Cost:10
  MD5 Authentication (Area) SPI 1000, secure socket state UP (errors:0)
  Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router (ID) 10.11.11.1, local address 2001:0DB1:A8BB:CCFF:FE00:6F00
  Backup Designated router (ID) 10.10.10.1, local address
FE80::A8BB:CCFF:FE00:6E00
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:03
  Index 1/1/1, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 10.11.11.1  (Designated Router)
  Suppress hello for 0 neighbor(s)
```

Examples

The following display shows sample output from the **showipv6ospfinterface** command when the OSPF cost dynamic is configured.

```
Router1# show ipv6 ospf interface serial 2/0
Serial2/0 is up, line protocol is up
```

```
   Link Local Address 2001:0DB1:A8BB:CCFF:FE00:100, Interface ID 10
   Area 1, Process ID 1, Instance ID 0, Router ID 172.1.1.1
   Network Type POINT_TO_MULTIPOINT, Cost: 64 (dynamic), Cost Hysteresis: 200
   Cost Weights: Throughput 100, Resources 20, Latency 80, L2-factor 100
   Transmit Delay is 1 sec, State POINT_TO_MULTIPOINT,
   Timer intervals configured, Hello 30, Dead 120, Wait 120, Retransmit 5
     Hello due in 00:00:19
   Index 1/2/3, flood queue length 0
   Next 0x0(0)/0x0(0)/0x0(0)
   Last flood scan length is 0, maximum is 0
   Last flood scan time is 0 msec, maximum is 0 msec
   Neighbor Count is 0, Adjacent neighbor count is 0
   Suppress hello for 0 neighbor(s)
```

Examples

The following display shows sample output from the **showipv6ospfinterface** command when the OSPF graceful restart feature is configured:

```
Router# show ipv6 ospf interface
Ethernet0/0 is up, line protocol is up
  Link Local Address FE80::A8BB:CCFF:FE00:300, Interface ID 2
  Area 0, Process ID 1, Instance ID 0, Router ID 10.3.3.3
  Network Type POINT_TO_POINT, Cost: 10
  Transmit Delay is 1 sec, State POINT_TO_POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
   Graceful Restart p2p timeout in 00:00:19
    Hello due in 00:00:02
  Graceful Restart helper support enabled
  Index 1/1/1, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 10.1.1.1
  Suppress hello for 0 neighbor(s)
```

Examples

The following display shows that the OSPF interface is enabled for Bidirectional Forwarding Detection (BFD):

```
Router# show ipv6 ospf interface
Serial10/0 is up, line protocol is up
  Link Local Address FE80::A8BB:CCFF:FE00:6500, Interface ID 42
  Area 1, Process ID 1, Instance ID 0, Router ID 10.0.0.1
  Network Type POINT_TO_POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT_TO_POINT, BFD enabled
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:07
  Index 1/1/1, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 10.1.0.1
  Suppress hello for 0 neighbor(s)
```

Related Commands

Command	Description
show ipv6 ospf graceful-restart	Displays OSPFv3 graceful restart information.

show mcsa statistics

To display the mobile client service abstraction (MCSA) notification statistics, use the **show mcsa statistics** command in privileged EXEC mode.

show mcsa statistics{**sint**| **cint**}

Syntax Description

sint	Specifies the service interface notification statistics.
cint	Specifies client interface notification statistics.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.8S	This command was introduced

Usage Guidelines

Enable MCSA by using the **mcsa** command before you enter the **show mcsa statistics** command.

Examples

The following is sample output from the **show mcsa statistics sint** command:

```
Device# show mcsa statistics sint

Session Create Req              : 1
Session Create Res              : 1
Session Update Req              : 0
Session Update Res              : 0
Session Update Ind              : 0
Session Update Rep Success      : 0
Session Update Rep Failed       : 0
Session Delete Req              : 0
Session Delete Res              : 0
Session Delete Ind              : 0
Session Delete Rep Success      : 0
Session Delete Rep Failed       : 0
```

The following is sample output from the **show mcsa statistics cint** command:

```
Device# show mcsa statistics cint

Protocol : PMIPV6
Set Interest list               : 1
Attach Indication               : 1
Attach Rep Success              : 1
Attach Rep Failed               : 0
Detach Indication               : 0
Detach Rep Success              : 0
Detach Rep Failed               : 0
Cleanup Req                     : 0
Cleanup Res                     : 0
```

```
Attach Update Req                : 0
Attach Update Res                : 0
Attach Update Ind                : 0
Attach Update Rep Success        : 0
Attach Update Rep Failed         : 0

Protocol : GTP

Set Interest list                : 1
Attach Indication                : 0
Attach Rep Success               : 0
Attach Rep Failed                : 0
Detach Indication                : 0
Detach Rep Success               : 0
Detach Rep Failed                : 0
Cleanup Req                      : 0
Cleanup Res                      : 0
Attach Update Req                : 0
Attach Update Res                : 0
Attach Update Ind                : 0
Attach Update Rep Success        : 0
Attach Update Rep Failed         : 0
```

Related Commands

Command	Description
mcsa	Enables the MCSA.
clear mcsa statistics	Clears the MCSA notifications statistics.

show mux

To display general IP multiplexing information, use the **show mux** command in user EXEC or privileged EXEC mode.

show {**ip**| **ipv6**} **mux**

Syntax Description

ip	Displays IPv4 multiplexing information.
ipv6	Displays IPv6 multiplexing information.

Command Modes

User EXEC

Privileged EXEC

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.

Examples

The following example shows how to display IP multiplexing statistics:

```
Router# show ip mux
IPv4 Multiplexing
  Superframe UDP Port: 6682

Multiplexing Policies
 muxpol             Outbound DSCP:     19
                     Match DSCP values: af21 19
 muxpol2            Outbound DSCP:     af11
                     Match DSCP values: 11
 muxpol3            Outbound DSCP:     2
                      Match DSCP values: 1

IPv4 Multiplex Cache Statistics
  Current Entries:                3
  Maximum Number of Entries:       56818
  Cache High Water Mark:           3
  Total Stale Entries:             0
  Total Do-Not-Multiplex Entries: 0
Router#
```

The table below describes the significant fields shown in the display.

Table 33: show mux Field Descriptions

Field	Description
Superframe UDP Port	UDP port configured for IP multiplexing.
Multiplexing Policies	List of each configured IP multiplexing policy with the policy name, configured outbound differentiated services code point (DSCP) value, and DSCP values in packets bound for multiplexing.
Current Entries	Number of entries listed in the IP multiplexing cache.
Maximum Number of Entries	Maximum number of entries that the cache can contain.
Cache High Water Mark	Maximum number of entries that have ever been in the cache at one time. This value might not represent the current number of entries in the cache.
Total Stale Entries	An entry in the cache that is older than 30 seconds and has not been referenced. Every 30 seconds, any unreferenced entry older than 30 seconds is marked stale. Stale entries are deleted from the cache. If the cache is full, stale entries are overwritten first.
Total Do-Not-Multiplex Entries	Number of entries in the cache designated to not multiplex.

show mux cache

To display IP multiplexing cache statistics, use the **show mux cache** command in user EXEC or privileged EXEC mode.

show {**ip**| **ipv6**} **mux cache** [**profile** *profile-name*| **nomux**| **stale**]

Syntax Description

ip	Displays IPv4 multiplexing cache statistics.
ipv6	Displays IPv6 multiplexing cache statistics.
profile *profile-name*	(Optional) Displays IP multiplexing cache contents by profile.
nomux	(Optional) Displays IP multiplexing cache of do-not-multiplex entries.
stale	(Optional) Displays IP multiplexing cache stale entries.

Command Modes

User EXEC

Privileged EXEC

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.

Examples

The following example shows how to display the IPv6 multiplexing cache statistics:

```
Router# show ipv6 mux cache
IPv6 Multiplex Cache Statistics

Current Entries:                  2
  Maximum Number of Entries:      9615
  Cache High Water Mark:          2
  Total Stale Entries:            0
  Total Do-Not-Multiplex Entries: 2
IPv6 Multiplex Cache Contents

Destination Address                     Port      Protocol    DSCP     Profile
------------------------------------------------------------------------------
200:200:200:200:200:0:E01:5600          0         UDP         1        r1v6
200:200:200:200:200:0:E01:5600          0         UDP         af11     No mux
Router#
```

The table below describes the significant fields shown in the display.

Table 34: show mux cache Field Descriptions

Field	Description
Current Entries	Number of entries listed in the IP multiplexing cache.
Maximum Number of Entries	Maximum number of entries that the cache can hold.
Cache High Water Mark	Maximum number of entries that have ever been stored in the cache. If this value varies significantly from the maximum number of cache entries, consider changing the cache size.
Total Stale Entries	An entry in the cache that is older than 30 seconds and has not been referenced. Every 30 seconds, any unreferenced entry older than 30 seconds is marked stale. Stale entries are deleted from the cache. If the cache is full, stale entries are overwritten first.
Total Do-Not-Multiplex Entries	Number of entries in the cache designated to not multiplex.
Destination Address	Destination IPv4 or IPv6 address for the cache entry.
Port	Port configured for the cache entry.
Protocol	Protocol configured for the cache entry.
DSCP	Differentiated services code point.
Profile Name	Name of the profile

The following example shows how to display the cache statistics for do-not-multiplex entries:

```
Router# show ip mux cache nomux
IPv4 Multiplex Cache
Destination Address    Port    Protocol    DSCP    Profile
----------------------------------------------------------
192.0.2.1                0       ICMP        0       No mux
Router#
```

The following example shows how to display the cache statistics for stale entries:

```
Router# show ip mux cache stale
IPv4 Multiplex Cache
Destination Address    Port    Protocol    DSCP    Profile
----------------------------------------------------------
192.0.2.21            1000    UDP         1       r1 (stale)
192.0.2.21            1000    UDP         af12    r1 (stale)
Router#
```

The following example shows how to display the cache statistics for the IP multiplexing profile r1:

```
Router# show ip mux cache profile r1

IPv4 Multiplex Cache

Destination Address    Port    Protocol    DSCP    Profile
----------------------------------------------------------
192.0.2.20             0       ICMP        0       r1
192.0.2.21             1000    UDP         1       r1 (stale)
192.0.2.21             1000    UDP         af12    r1 (stale)
192.0.2.20             1001    UDP         af21    r1
Router#
```

show mux interface

To display configured IP multiplexing statistics for an interface, use the **show mux interface** command in user EXEC or privileged EXEC mode.

show {**ip**| **ipv6**} **mux interface** [*type*]

Syntax Description

ip	Displays IPv4 multiplexing statistics.
ipv6	Displays IPv6 multiplexing statistics.
type	(Optional) Interface type. These interface types are valid: • Ethernet: IEEE 802.3 • Tunnel: Tunnel interface • Virtual-Template: Virtual template interface • VMI: Virtual multipoint interface

Command Modes

User EXEC

Privileged EXEC

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 interface type, the **show mux interface** command displays statistics for all interfaces with IP multiplexing configured.

Examples

The following example shows how to display IP multiplexing statistics for Ethernet 0/1:

```
Router# show ip mux interface Ethernet0/1
IP multiplexing statistics for Ethernet0/1:
  Transmit:
   IPv4 superframes transmitted: 20430
   IPv4 packets multiplexed:    30555
   Average TX mux ratio:        1.49:1
  Receive:
   IPv4 superframes received:   22009
   IPv4 packets demuxed:        32634
   IPv4 format errors:          0
   Average RX mux ratio:        1.48:1
Router#
```

The table below describes the significant fields shown in the display.

Table 35: show mux interface Field Descriptions

Field	Description
IPv4 super frames transmitted	Number of IPv4 superframes transmitted from the interface.
IPv4 packets multiplexed	Number of packets that have been processed and put into superframes.
Average TX mux ratio	Ratio of the total number of packets put into superframes divided by the number of superframes transmitted.
IPv4 superframes received	Number of IPv4 superframes received over the interface.
IPv4 packets demuxed	Number of IPv4 packets demultiplexed from received superframes.
IPv4 format errors	Number of packets with format errors after they have been demultiplexed.
Average RX mux ratio	Ratio of the total number of successfully demultiplexed packets divided by the number of superframes received.

show mux profile

To display multiplexing statistics and the configuration for a specific IP multiplexing profile, use the **show mux profile** command in user EXEC or privileged EXEC mode.

show {**ip**| **ipv6**} **mux profile** [*profile-name*]

Syntax Description

ip	Displays IPv4 multiplexing cache statistics.
ipv6	Displays IPv6 multiplexing cache statistics.
profile-name	(Optional) Name of the IP multiplexing profile.

Command Modes

User EXEC

Privileged EXEC

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 IP multiplexing profile name, this command displays the statistics for all configured profiles.

Examples

The following example shows how to display the cache statistics for the IPv6 profile r1v6:

```
Router# show ipv6 mux profile rlv6
Profile r1v6
  Shutdown:                     No
  Destination:                  2000:0:1:2:A8BB:CCFF:FE01:5610
  Source:                       2000:0:1:1:A8BB:CCFF:FE01:5510  (Ethernet0/1)
  Access-list:                  muxv6acl
  TTL:                          64
  Max mux length:               1452
  MTU:                          1500
  Hold time(ms):                20
  Single packet superframes:    Enabled
  Inbound (demux) Statistics
    Superframes received:          0
    Packets demultiplexed:         0
    Avg. Inbound Multiplex ratio: N/A
  Outbound (mux) Statistics
  Default Policy
    Packets: 0/0  Full Superframes: 0  Partial Superframes: 0
    Avg. Outbound Multiplex ratio: N/A     Mux length exceeded: 0
  Policy dscp4
    Packets: 3963/3616  Full Superframes: 0  Partial Superframes: 984
    Avg. Outbound Multiplex ratio: 3.67:1     Mux length exceeded: 0
Router#
```

The table below describes the significant fields shown in the display.

Table 36: show ipv6 mux profile Field Descriptions

Field	Description
Profile	Name of the configured IP multiplexing profile.
Shutdown	Current state of the profile. • No—the profile is enabled. • Yes—the profile is disabled.
Destination	Destination IPv4 or IPv6 address configured for the profile.
Source	Source IPv4 or IPv6 address configured for the profile.
Access-list	Name of the access list used by the IP multiplexing profile.
TTL	Configured time-to-live (TTL) value for outbound superframes. Number of hops before the superframe expires.
Max mux length	Maximum packet size that the multiplex profile can hold for multiplexing.
MTU	Maximum transmission unit (MTU) size for an outbound superframe.
Holdtime (ms)	Length of time IP multiplexing waits after not having not received a packet before sending the superframe.
Single packet superframes	• Enabled—Superframes with only one packet are sent. • Disabled—Single packets are not sent as superframes.
Inbound (demux) Statistics	
Superframes received	Number of superframes the IP multiplexing policy has received.

Field	Description
Packets demultiplexed	Number of packets that have been demultiplexed from superframes.
Avg. Inbound Multiplex ratio	Number of inbound packets demultiplexed divided by the number of superframes received.
Outbound (mux) Statistics (listed by policy name)	
Packets	The first value is the number of outbound packets processed by the policy. The second value is the number of packets that were transmitted inside superframes.
Full Superframes	Number of full superframes that the policy has sent.
Partial Superframes	Number of partial superframes the policy has sent.
Avg. Outbound Multiplex ratio	Ratio of the number of packets processed by the policy divided by the number of full superframes and partial superframes sent by the policy.
Mux length exceeded	Number of packets processed by the policy that exceed the configured maximum packet length.

show vmi neighbors

To display information about neighbor connections to the Virtual Multipoint Interface (VMI), use the **show vmi neighbors** command in user and in privileged EXEC mode.

show vmi neighbors [detail] [*vmi-interface*]

Syntax Description

detail	(Optional) Displays details about the VMI neighbors.
vmi-interface	(Optional) Number of the VMI interface

Command Default

If no arguments are specified, information about all neighbors for all VMI interfaces is displayed.

Command Modes

User EXEC Privileged EXEC

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.
15.1(3)T	This command was modified. When the **detail** keyword is used, the output is enhanced with additional PPPoE flow control statistics.

Usage Guidelines

If no arguments are specified, information about all neighbors for all VMI interfaces is displayed.

The **show vmi neighbors**command provides a list of devices that have been dynamically discovered by the connected radio devices in a router-to-radio network, and for which connectivity has been achieved through PPPoE and the radio network.

Examples

The following is sample output from the **show vmi neighbors** command used to display dynamically created neighbors on a VMI interface.

```
Router# show vmi neighbors vmi1
1 vmi1 Neighbors
           IPV6       IPV4                          Transmit    Receive
Interface  Address    Address       Uptime      Packets     Packets
vmi1       ::         10.3.3.2      00:02:11    0000000008  0000000073
```

Below table describes the significant fields shown in the **show vmi neighbors** command display.

Table 37: show vmi neighbors Field Descriptions

Field	Description
Interface	The interface number.
IPv6 Address	IPv6 address of the neighbor.
IPv4 Address	IPv4 address of the neighbor.
Uptime	How long the interface has been up. Time shown in hh:mm:ss format.
Transmit Packets	Number of packets transmitted from the interface during the monitored up time.
Received Packets	Number of packets received on the interface during the monitored up time.

Examples

The following example shows the details about the known VMI neighbors.

```
Router# show vmi neighbors detail

1 vmi1 Neighbors
vmi1   IPV6 Address=::
       IPV4 Address=10.3.3.2, Uptime=00:02:16
       Output pkts=8, Input pkts=75
       No Session Metrics have been received for this neighbor.
       Transport PPPoE, Session ID=79
       INTERFACE STATS:
          VMI Interface=vmi1,
             Input qcount=0, drops=0, Output qcount=0, drops=0
          V-Access intf=Virtual-Access3,
             Input qcount=0, drops=0, Output qcount=0, drops=0
          Physical intf=FastEthernet0/0,
             Input qcount=0, drops=0, Output qcount=0, drops=0
PPPoE Flow Control Stats
 Local Credits: 65524   Peer Credits: 65524   Scalar Value 64 bytes
 Credit Grant Threshold: 28000    Max Credits per grant: 65534
 Credit Starved Packets: 0
 PADG Seq Num: 24     PADG Timer index: 0
 PADG last rcvd Seq Num: 24
 PADG last nonzero Seq Num: 0
 PADG last nonzero rcvd amount: 0
 PADG Timers:    [0]-1000    [1]-2000    [2]-3000    [3]-4000
 PADG xmit: 24  rcvd: 24
 PADC xmit: 24  rcvd: 24
 PADQ xmit: 0  rcvd: 0
```

The below table describes the significant fields shown in the **show vmi neighbors detail**command display.

Table 38: show vmi neighbors detail Field Descriptions

Field	Description
Interface	The interface number.
IPv6 Address	IPv6 address of the neighbor.

Field	Description
IPv4 Address	IPv4 address of the neighbor.
Uptime	How long the interface has been up. Time shown in hh:mm:ss format.
Output pkts	Number of outgoing packets during the recorded up time.
Input pkts	Number of incoming packets during the recorded up time.
Metric Data	The Metric data statistics Total rcvd: The total number of packets received on the interface Avg arrival rate: The average arrival rate for each packet in milliseconds. CURRENT: The current values for the following statistics: metric data rate (MDR), credit data rate (CDR), latency (Lat), resource (Res), RLQ (RLQ), and the load MDR: The maximum, minimum, and average metric data rate CDR: The maximum, minimum, and average credit data rate Latency: The maximum, minimum, and average latency Resource: The maximum, minimum, and average resource RQL: The maximum, minimum, and average RQL Load: The maximum, minimum, and average load
Transport	The routing protocol, in this case-PPPoE.
Session ID	The identifier of the VMI session.
INTERFACE STATS	A series of statistics collected on the interface and shows for each of the VMI interface, virtual access interface, and the physical interface. For each interface, statistics are displayed indicating the number of packets in the input and output queues and the number of packets dropped from each queue.

Field	Description
PPPoE Flow Control Stats	The statistics collected for PPPoE credit flow. **Local Credits** : The number of credits belonging to this node.**Peer Credits**: The number of credits belonging to the peer. Scalar Value: The credit grant in bytes specified by the radio**Credit Grant Threshold**: The number of credits below which the peer needs to dip before this node sends an inband or out-of-band grant. Credit Starved Packets: The number of packets dropped or queued due to insufficient credits from the peer.**Max Credits per grant**: 65534**PADG Seq Num**: The sequence number for the PPPoE packet discovery grant**PADG Timer index**: The timer index for the PPPoE packet discovery grant**PADG last rcvd Seq Num**: The sequence number for the previously received PPPoE packet discovery grant**PADG last nonzero Seq Num**: The sequence number for the last non-zero PPPoE packet discovery grant**PADG last nonzero rcvd amount**: The received amount in the last non-zero PPPoE packet discovery grant**PADG Timers**: The PPPoE packet discovery grant timers**PADG xmit**: *numeric* **rcvd**: The number of PPPoE packet discovery grants transmitted and received**PADC xmit**: **133 rcvd: 133:**The number of PPPoE packet discovery grant confirmations transmitted and received**PADQ xmit**: **0 rcvd**: The number of PPPoE packet discovery quality grants transmitted and received.

Related Commands

Command	Description
debug vmi	Displays debugging output for VMIs.
interface vmi	Creates a VMI that can be configured and applied dynamically.

shutdown (IP multiplexing)

To deactivate an IP multiplexing profile, use the **shutdown** command in IPv4 multiplexing profile configuration or IPv6 multiplexing profile configuration mode. To activate an IP multiplexing profile, use the no form of this command.

shutdown

no shutdown

Syntax Description

This command has no arguments or keywords.

Command Default

The IP multiplexing profile is activated.

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

You must enter the **no shutdown** command to activate an IP multiplexing profile so that the IP multiplexing packet handler processes packets for IP multiplexing. A disabled multiplexing profile cannot send superframes but will accept incoming superframes that match its configured source and destination addresses.

If you want to change the access control list (ACL) associated with the profile, or edit the ACL associated with the profile, you must enter the **shutdown** command. After you have changed either the access list or the ACL associated with the profile, you then enter the **no shutdown** command to clear the IP multiplexing cache and use the new information.

A source and destination address must be configured for a multiplexing profile before it can be activated.

Examples

The following example shows how to deactivate the IP multiplexing profile routeRTP-SJ:

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

singlepacket

To enable the IP multiplexing packet handler to send single-packet superframes, use the **singlepacket** command in IPv4 multiplexing profile configuration or IPv6 multiplexing profile configuration mode. To prevent the creation of single-packet superframes, use the **no** form of this command.

singlepacket

no singlepacket

Syntax Description

This command has no arguments or keywords.

Command Default

Single-packet superframes are not sent.

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

By default, the IP multiplexing packet handler creates single-packet superframes.

Single-packet multiplexing applies to all hold queues for a given IP multiplexing profile.

Interesting data packets are always transmitted inside a superframe even if there is only one packet to transmit when the hold timer expires.

Examples

The following example shows how to configure single-packet superframes for IP multiplexing profile *routeRTP-SJ* :

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

snmp-server enable traps ipmobile

To enable Simple Network Management Protocol (SNMP) security notifications for Mobile IP, use the **snmp-server enable traps ipmobile**commandin global configuration mode. To disable SNMP notifications for Mobile IP, use the **no**form of this command.

snmp-server enable traps ipmobile

no snmp-server enable traps ipmobile

Syntax Description

This command has no arguments or keywords.

Command Default

SNMP notifications are disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.

Usage Guidelines

SNMP Mobile IP notifications can be sent as traps or inform requests. This command enables both traps and inform requests. This command enables Mobile IP Authentication Failure notifications. This notification is defined in RFC2006-MIB.my as the mipAuthFailure notification type {mipMIBNotifications 1}. This notification, when enabled, is triggered when there is an authentication failure for the Mobile IP entity during validation of the mobile registration request or reply.

For a complete description of this notification and additional MIB functions, see the RFC2006-MIB.my file, available on Cisco.com at http://www.cisco.com/public/mibs/v2/.

The **snmp-server enable traps ipmobile**command is used in conjunction with the **snmp-server host**command. Use the **snmp-server host** global configuration command to specify which host or hosts receive SNMP notifications. To send SNMP notifications, you must configure at least one **snmp-server host**command.

Examples

The following example enables the router to send Mobile IP informs to the host at the address myhost.cisco.com using the community string defined as public:

```
snmp-server enable traps ipmobile
snmp-server host myhost.cisco.com informs version 2c public
```

Related Commands

Command	Description
snmp-server host	Specifies the recipient of an SNMP notification operation.

Command	Description
snmp-server trap-source	Specifies the interface from which an SNMP trap should originate.

source (IP multiplexing)

To specify the IPv4 or IPv6 source address for the local endpoint of an IP multiplexing path, use the **source** command in IPv4 multiplexing profile configuration or IPv6 multiplexing profile configuration mode. To clear the source address, use the **no** form of the command.

source {*ip-addr*| *ipv6-addr*| **interface** *type*}

no source

Syntax Description

ip-addr	IPv4 source address for the local endpoint of the IP multiplexing path.
ipv6-addr	IPv6 source address for the local endpoint of the IP multiplexing path.
interface *type*	Physical interface for the source local endpoint of the IP multiplexing path.

Command Default

Source addresses are not specified.

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

You must configure a source address for the profile in order to use it. If you attempt to issue a **no shutdown** command when no source address is configured, you are prompted to configure a source address. If a profile is active, you must issue a **shutdown** command before changing the source address.

After you specify the source address, if you enter the **source** command again, the new address overwrites the previously entered address.

Before a superframe can be demultiplexed, an incoming superframe must match its source and destination addresses to the destination and source addresses, respectively, in the multiplexing profile. If either address does not match, the superframe is ignored.

Examples

The following example shows how to configure an IPv6 address as the source address for superframe packets:

```
Router# configure terminal
Router(config)# ipv6 mux profile routeRTP-SJ
Router(config-ipmux-profile-v6)# source FE80::A8BB:CCFF:FE01:5700
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.

template tunnel (mobile networks)

To apply a tunnel template to tunnels brought up at the home agent, use the **template tunnel**command in mobile networks configuration mode. To remove the tunnel template, use the **no** form of this command.

template tunnel *interface-number*

no template tunnel *interface-number*

Syntax Description

interface-number	Tunnel interface number.

Command Default

No default behavior or values

Command Modes

Mobile networks configuration

Command History

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

Usage Guidelines

This command allows the configuration of multicast on statically created tunnels to be applied to dynamic tunnels brought up on the home agent.

Examples

The following example shows the template tunnel applied at the home agent:

```
! Tunnel template to be applied to mobile networks
interface tunnel 100
 ip pim sparse-mode
!
! Select tunnel template to apply during registraton
ip mobile mobile-networks 10.1.0.1
 template tunnel 100
```

Related Commands

Command	Description
template tunnel (mobile router)	Applies a tunnel template to tunnels brought up at the mobile router.

template tunnel (mobile router)

To apply a tunnel template to tunnels brought up at the mobile router, use the **template tunnel**command in mobile router configuration mode. To remove the tunnel template, use the **no** form of this command.

template tunnel *interface-number*

no template tunnel *interface-number*

Syntax Description

interface-number	Tunnel interface number.

Command Default

No default behavior or values

Command Modes

Mobile router configuration

Command History

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

Usage Guidelines

This command allows the configuration of multicast on statically created tunnels to be applied to dynamic tunnels brought up on the mobile router.

Examples

The following example shows the template tunnel applied at the mobile router:

```
! Tunnel template to be applied to mobile networks
interface tunnel100
 ip pim sparse-mode
!
! Select tunnel template to apply during registration
ip mobile router
 template tunnel100
```

Related Commands

Command	Description
template tunnel (mobile networks)	Applies a tunnel template to tunnels brought up at the home agent.

ttl (IP multiplexing)

To insert into the superframe header the time-to-live (TTL) value for outbound superframes, use the **ttl** 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.

ttl *hops*

no ttl

Syntax Description

hops	Number of hops equivalent to the TTL value inserted into the IP header of the outbound superframe. The range is 1 to 255.

Command Default

The TTL is 64 hops.

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 TTL, the IP multiplexing packet handler uses the default value of 64 hops.

After you specify the TTL value, if you enter the **ttl** command again, the new TTL value overwrites the previously entered size.

Examples

The following example shows how to configure the TTL size for an IP multiplexing profile to 255 hops:

```
Router# configure terminal
Router(config)# ipv6 mux profile routeRTP-SJ
Router(config-ipmux-profile-v6)# ttl 255
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.

tunnel mode gre

To set the global encapsulation mode on all roaming interfaces of a mobile router to generic routing encapsulation (GRE), use the **tunnel mode gre**command inmobile router configuration mode. To restore the global default encapsulation mode, use the **no** form of this command.

tunnel mode gre

no tunnel mode gre

Syntax Description

This command has no arguments or keywords.

Command Default

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

Command Modes

Mobile router configuration

Command History

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

Usage Guidelines

If the **tunnel mode gre** command is configured, the mobile router will try to register with the foreign agent (FA) with the G bit set if the FA advertises GRE. If the registration request is successful, packets will be routed using GRE.

If the **tunnel mode gre** command is enabled and collocated care-of address (CCoA) is configured, the mobile router will try to register with the home agent (HA) with the G bit set. If the registration request is successful, packets will be routed 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 tunnel mode gre**command instructs the mobile router to revert to the default 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 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, reregistration will be attempted.

Examples

The following example globally configures GRE encapsulation on a mobile router and enables GRE keepalive messages:

```
router mobile
!
ip mobile secure home-agent 10.40.40.1 spi 101 key hex 12345678123456781234567812345678
   algorithm md5 mode prefix-suffix
ip mobile router
 address 10.80.80.1 255.255.255.0
 home-agent 10.40.40.1
 mobile-network Ethernet1/3
 mobile-network FastEthernet0/0
 template Tunnel 121
 tunnel mode gre
!
interface tunnel 121
 keepalive 5 3
```

Related Commands

Command	Description
ip mobile router-service tunnel mode gre	Sets the encapsulation mode to GRE for a mobile router interface.
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 mtu

To specify a maximum transmission unit (MTU) to be applied on the Proxy mobile IPv6 (PMIPv6) tunnel in a Local Mobility Anchor (LMA), use the **tunnel mtu** command in LMA configuration mode. To remove MTU specification, use the **no** form of this command.

tunnel mtu *value*

no tunnel mtu

Syntax Description

value	Value of the MTU.

Command Default

The default MTU value will be applied on the PMIPv6 tunnel.

Command Modes

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

Command History

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

Examples

The following example shows how to provide the IPv6 service to the mobile node (MN):

```
Device(config)# ipv6 mobile pmipv6-lma lma1 domain d1
Device(config-ipv6-pmipv6-lma)# tunnel mtu 1360
```

tunnel nat

To designate that traffic originating from or destined to the Proxy Mobile IPv6 (PMIPv6) tunnel is subject to Network Address Translation (NAT), use the **tunnel nat** command in MAG configuration mode. To prevent the PMIPv6 tunnel from being able to translate, use the **no** form of this command.

tunnel nat {*inside*| *outside*}

no tunnel nat {*inside*| *outside*}

Syntax Description

inside	Indicates that the interface is connected to the inside network which is subject to NAT translation.
outside	Indicates that the interface is connected to the outside network.

Command Default

The traffic originating from or destined to the PMIPv6 tunnel is not subject to NAT.

Command Modes

MAG configuration (config-ipv6-pmipv6-mag)

Command History

Release	Modification
15.4(1)T	This command was introduced.

Examples

The following example shows how to specify NAT for a PMIPv6 tunnel in MAG:

```
Device(config)# ipv6 mobile pmipv6-mag mag1 domain d1
Device(config-ipv6-pmipv6-mag)# tunnel nat outside
```

Related Commands

Command	Description
ip nat	Designates that traffic originating from or destined for the interface is subject to NAT.

vrfid (proxy mobile IPv6)

To specify a Virtual Private Network (VPN) Route Forwarding (VRF) for a local mobility access (LMA) peer that is configured under a mobile access gateway (MAG), use the **vrfid** command in MAG-LMA configuration mode. To disassociate a VRF from an LMA peer that is configured under a MAG, use the **no** form of this command.

vrfid

no vrfid

Syntax Description

This command has no arguments or keywords.

Command Default

No VRF is specified for an LMA peer that is configured under a MAG.

Command Modes

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

Command History

Release	Modification
Cisco IOS XE Release 3.8S	The command was introduced.

Usage Guidelines

This command is not supported in standalone MAG configuration. Use this command only when a MAG is configured to coexist with the Intelligent Services Gateway (ISG). Configure a VRF routing table instance using **vrf definition** command prior to using the **vrfid** command.

Examples

The following example shows how to specify a VRF for an LMA peer that is configured under a MAG:

```
Device# enable
Device# configuration terminal
Device(config)# vrf definition vrf1
Device(config-vrf)# rd 100:20
Device(config-vrf)# exit
Device(config)# ipv6 mobile pmipv6-mag mag1 domain dn1
Device(config-ipv6-pmipv6-mag)# lma lma1
Device(config-ipv6-pmipv6mag-lma) vrfid vrf1
Device(config-ipv6-pmipv6mag-lma) end
```

Related Commands

Command	Description
vrf definition	Configures a VRF table instance.