

nai (proxy mobile ipv6)

To configure the Network Access Identifier (NAI) for the mobile node (MN) within the Proxy Mobile IPv6 (PMIP) domain, use the **nai** command in PMIP domain configuration mode. To disable the NAI configuration, use the **no** form of this command.

```
nai [user]@realm
```

```
no nai [user]@realm
```

Syntax Description

<i>user@realm</i>	Qualified specific user address and domain. The @ symbol is required.
<i>@realm</i>	Any user address at a specific realm. The @ symbol is required.

Command Default

The NAI for the MN is not specified.

Command Modes

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

Command History

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

Examples

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

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

Related Commands

Command	Description
ipv6 mobile pmipv6-domain	Configures the PMIP 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

<i>net</i>	IP address of the directly connected networks.
<i>mask</i>	Network mask.

Defaults

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:

Mobile Router Configuration

```
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
```

Home Agent Configuration

```
! 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.

physical-interface

To create a physical subinterface to be associated with the Virtual Multipoint Interfaces (VMI) on a router, use the **physical-interface** command in interface configuration mode. To return the interface to the default mode of synchronous, use the **no** form of this command.

physical-interface *interface-type/slot*

no physical-interface

Syntax Description

<i>interface-type</i>	The type of interface or subinterface; value can be Ethernet, Fast Ethernet, or Gigabit Ethernet. The slash mark (/) is required between the interface and slot values.
<i>slot</i>	Indicates the slot in which the interface is present.

Defaults

No physical interface exists until created.

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 Virtual Multipoint Interfaces (VMIs) in Mobile Adhoc Router-to-Radio Networks

Usage Guidelines

Use the **physical-interface** command to create a physical subinterface.

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 change a low-speed serial interface from synchronous to asynchronous mode:

```
Router(config)# interface vmi1
Router(config-if)# physical-interface fe0/1
```

Related Commands

Command	Description
debug vmi	Displays debugging output for virtual multipoint interfaces (VMIs)
eigrp interface	Sets a threshold value to minimize hysteresis in a router-to-radio configuration.

Command	Description
interface vmi	Creates a VMI interface.
mode bypass	Enables Virtual Multipoint Interfaces (VMI) to support multicast traffic

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	<i>name</i>	Name of the mobile router group.
--------------------	-------------	----------------------------------

Defaults	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 fault tolerance by selecting one mobile router in the redundancy group <i>name</i> 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.

Defaults 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 control the registration parameters of the mobile router, use the **register** command in 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		Re-registers before the lifetime expires.
expire <i>seconds</i>		Time (in seconds) in which to send a registration request before expiration. The range is from 1 to 3600; the default is 120.
retry <i>number</i>		Number of times the mobile router retries sending a registration request if no reply is received. 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 <i>seconds</i>		Time (in seconds) that the mobile router waits before sending another registration request if no reply is received. The range is from 1 to 3600; the default is 10.
lifetime <i>seconds</i>		Requested lifetime (in seconds) of each registration. The smallest value between the configured lifetime and the foreign agent advertised registration lifetime is used. The range is from 3 to 65534; default is 65534 (infinity). This default ensures that the advertised lifetime is used, excluding infinity.
retransmit initial <i>milliseconds</i>		Wait period (in milliseconds) before sending a retransmission the first time no reply is received from the foreign agent. The range is from 10 to 10000 milliseconds (10 seconds); the default is 1000 milliseconds (1 second).
maximum <i>milliseconds</i> retry <i>number</i>		Maximum wait period (in milliseconds) before retransmission of a registration request. The range is 10 to 10000 milliseconds (10 seconds); the default is 5000 milliseconds (5 seconds). Each successive retransmission timeout period is twice the previous period, as long as it is less than the maximum value. Retransmission stops after the maximum number of retries.

Defaults

expire *seconds*: 120 seconds
retry *number*: Three retries
interval *seconds*: 10 seconds
lifetime *seconds*: 65534 seconds
retransmit initial *milliseconds*: 1000 milliseconds (1 second)
maximum *milliseconds*: 5000 milliseconds (5 seconds)

Command Modes

Mobile router configuration

Command History

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

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
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.

replay-protection

To configure the replay protection mechanism within the Proxy Mobile IPv6 (PMIP) domain, or the Mobile Access Gateway (MAG), use the **replay-protection** command in PMIP domain or MAG 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 timestamp.
	window <i>seconds</i>	(Optional)Specifies the maximum amount of 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 1 to 255.

Command Default The replay protection mechanism is configured with the time stamp default window period as 7 seconds.

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 The window period is the maximum amount of 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 timestamp** command in PMIP domain configuration mode to configure the replay protection mechanism. If the PMIP 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.

The **no replay-protection timestamp** command sets the time stamp window period to 7 seconds.

Examples The following example shows how to configure replay protection mechanism with a window period of 200 seconds within the PMIP domain:

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

```
Router(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:

```
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)# no replay-protection timestamp
```

Related Commands

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

Defaults 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.

role

To configure the role of the Mobile Access Gateway (MAG), use the **role** command in MAG configuration mode. To remove the role of the MAG, 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 3rd 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.

Usage Guidelines

The default role WLAN cannot be disabled, but can be reconfigured to 3GPP, LTE, or WiMAX. The **no role {3gpp | lte | wimax}** command will reset the role of the MAG to WLAN.



Note In Cisco IOS XE Release 3.4, 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:

```
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)# role 3gpp
```

Related Commands

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

Defaults 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.

service (proxy mobile ipv6)

To configure the service provided to the mobile node (MN) within the Proxy Mobile IPv6 (PMIP) domain, use the **service** command in mobile node configuration mode. To reset the service configuration to IPv4, use the **no** form of this command.

```
service ipv4
```

```
no service ipv4
```

Syntax Description

ipv4	Specifies the IPv4 service to the MN.
-------------	---------------------------------------

Command Default

The IPv4 service is provided to the MN.

Command Modes

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

Command History

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

Examples

The following example shows how to provide the IPv4 service to the MN:

```
Router(config)# ipv6 mobile pmipv6-domain dn1
Router(config-ipv6-pmipv6-domain)# nai example@abc.com
Router(config-ipv6-pmipv6-domain-mn)# service ipv4
```

Related Commands

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

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	
<i>ip-address</i>	(Optional) IP address of the mobile node (MN).
nai <i>network-address-id</i>	(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).
<i>ip-address</i>	(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 <i>string</i> 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 <i>ip-address</i> 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.
	12.4(24)T	The output was enhanced to display link-type labels.

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 3
192.0.2.0(Bindings 3):
  Care-of Addr 192.0.2.102, Src Addr 192.0.2.102
  Lifetime granted 00:01:30 (90), remaining 00:00:53
  Flags sbdmg-T-, Identification CD1E860C.46A7467C
  Tunnel0 src 192.0.2.3 dest 192.0.2.102 reverse-allowed
  MR Tunnel1 src 192.0.2.3 dest 192.0.2.0 reverse-allowed
  Routing Options - (T)Reverse-tunnel
  Mobile Networks: 209.165.200.225/255.255.255.224 (D)
  Roaming IF Attributes: BW 10000 Kb, ID 11
    Description WiMAX
  Metric bandwidth

192.0.2.0(Bindings 3):
  Care-of Addr 192.0.2.103, Src Addr 192.0.2.103
  Lifetime granted 00:01:30 (90), remaining 00:00:54
  Flags sbDmg-T-, Identification CD1E860D.4394D6C0
  Tunnel2 src 192.0.2.3 dest 192.0.2.103 reverse-allowed
  MR Tunnel2 src 192.0.2.3 dest 192.0.2.103 reverse-allowed
  Routing Options - (D)Direct-to-MN (T)Reverse-tunnel
  Mobile Networks: 209.165.200.225/255.255.255.224 (D)
  Roaming IF Attributes: BW 10000 Kb, ID 3, Link Type WIFI
  Metric bandwidth

192.0.2.0 (Bindings 3):
  Care-of Addr 192.0.2.104, Src Addr 192.0.2.104
  Lifetime granted 00:01:30 (90), remaining 00:01:19
  Flags sbdmg-T-, Identification CD1E8639.48B35C2C
  Tunnel3 src 192.0.2.3 dest 192.0.2.104 reverse-allowed
  MR Tunnel4 src 192.0.2.3 dest 192.0.2.0 reverse-allowed
  Routing Options - (T)Reverse-tunnel
  Mobile Networks: 209.165.200.225/255.255.255.224 (D)
  Roaming IF Attributes: BW 10000 Kb, ID 7, Link Type UMTS
  Metric bandwidth
```

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
192.0.2.6:
  Care-of Addr 192.0.2.7, Src Addr 192.0.2.7
  Lifetime granted 00:02:00 (120), remaining 00:01:56
  Flags sbDmgvT, Identification B7A262C5.DE43E6F4
  Tunnel0 src 10.0.0.3 dest 192.0.2.7 reverse-allowed
  MR Tunnel1 src 10.0.0.3 dest 192.0.2.6 reverse-allowed
  Routing Options - (D)Direct-to-MN (T)Reverse-tunnel
  Mobile Networks: 209.165.200.235/255.255.255.224(S)
  209.165.200.235/255.255.255.224 (D)
  209.165.200.235/209.165.200.255(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
192.0.2.10:
  Care-of Addr 192.0.2.20, Src Addr 192.0.2.27,
  Lifetime granted 00:33:20 (20000), remaining 00:30:56
  Flags SbdmGvt, Identification BC1C2A04.EA42659C,
  Tunnel0 src 192.0.2.207 dest 192.0.2.20 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 192.0.2.66
  Care-of Addr 192.0.2.107, Src Addr 192.0.2.119
  Lifetime granted 00:03:00 (180), remaining 00:02:20
  Flags sbDmg-T-, Identification BCF5F7FF.92C1006F
  Tunnel0 src 192.0.2.134 dest 192.0.2.119 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
192.0.2.178:
  Care-of Addr 192.0.2.172, Src Addr 192.0.2.172
  Lifetime granted 10:00:00 (36000), remaining 09:52:40
  Flags sbDmg-T-, Identification C5441314.61D36B14
  Tunnell src 192.0.2.249 dest 192.0.2.172 reverse-allowed
  MR Tunnell src 192.0.2.249 dest 192.0.2.172 reverse-allowed
  Routing Options - (D)Direct-to-MN (T)Reverse-tunnel
  Mobile Networks: 209.165.200.205/255.255.255.224 (D)
  Roaming IF Attributes: BW 10000 Kbit, ID 3247
  Description First Lan Interface
  Multi-path Metric bandwidth
```

[Table 9](#) 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.

Table 9 *show ip mobile binding Field Descriptions (continued)*

Field	Description
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.
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.
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.

Table 9 *show ip mobile binding Field Descriptions (continued)*

Field	Description
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

```

Table 10 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.

Table 10 *show ip mobile globals Field Descriptions (continued)*

Field	Description
Forced UDP Tunneling	Whether the home agent is configured to accept forced UDP tunneling.
Address	Home agent address.
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.
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.

Table 10 *show ip mobile globals Field Descriptions (continued)*

Field	Description
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 in privileged EXEC mode.

```
show ip mobile host [address | interface interface | network address | nai string | group [nai string] | summary]
```

Syntax Description		
<i>address</i>	(Optional) IP address of specific mobile node. If not specified, information for all mobile nodes is displayed.	
interface <i>interface</i>	(Optional) Displays all mobile nodes whose home network is on this interface.	
network <i>address</i>	(Optional) Displays all mobile nodes residing on this network or virtual network.	
nai <i>string</i>	(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

```

Table 11 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.
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)

```

Table 12 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 in privileged EXEC mode.

```
show ip mobile interface [interface]
```

Syntax Description	<i>interface</i> (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
```

[Table 13](#) 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.
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.

Table 13 *show ip mobile interface Field Descriptions (continued)*

Field	Description
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** command in privileged EXEC mode.

```
show ip mobile mobile-networks [ip-address]
```

Syntax Description	<i>ip-address</i>	(Optional) Address of a specific mobile router. If not specified, information for all mobile networks is displayed.
---------------------------	-------------------	---

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
```

[Table 14](#) 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:
```

```
MoIPProxyl@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 172.31.1.11
    On interface Ethernet3/0
    Tunnel3 mode GRE/IP

```

Table 15 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.
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.

Table 15 *show ip mobile router Field Descriptions (continued)*

Field	Description
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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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 in privileged EXEC mode.

show ip mobile router agent

Syntax Description This command has no arguments or keywords.

Defaults 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
```

show ip mobile router agent

```

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

```

Table 16 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.
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.
12.4(24)T	This command was enhanced to display link type labels.

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.

```
MR#show ip mobile router interface
```

```
Mobile Router Interfaces:
```

```
Listed in order of preference.
```

```
Ethernet2/0:
```

```
Priority 110, Bandwidth 10000, Address 57.0.0.1
Periodic solicitation disabled, Interval 600 sec
Retransmit Init 1000, Max 5000 msec, Limit 3
Current 2000, Remaining 0 msec, Count 2
Foreign agent hold down 0 sec
Layer 2 reassociation hold down 1000 msec
```

show ip mobile router interface

```

Last layer 2 link-state trap: None
Routing disallowed
Collocated CoA disabled
Interface ID 11
Interface description WiMAX

Ethernet1/0:
  Priority 110, Bandwidth 10000, Address 56.0.0.1
  Periodic solicitation disabled, Interval 600 sec
  Retransmit Init 1000, Max 5000 msec, Limit 3
  Current 2000, Remaining 0 msec, Count 2

Mobile Router Interfaces:

  Foreign agent hold down 0 sec
  Layer 2 reassociation hold down 1000 msec
  Last layer 2 link-state trap: None
  Routing disallowed
  Collocated CoA disabled
  Interface ID 7, Link type UMTS

Ethernet0/0:
  Priority 110, Bandwidth 10000, Address 55.0.0.1
  Periodic solicitation disabled, Interval 600 sec
  Retransmit Init 1000, Max 5000 msec, Limit 3
  Current 0, Remaining 0 msec, Count 0
  Foreign agent hold down 0 sec
  Layer 2 reassociation hold down 1000 msec
  Last layer 2 link-state trap: None
  Routing disallowed
  Collocated CoA 55.0.0.1
  UDP Tunneling disabled
  Interface ID 3, Link type WIFI

```

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

```

[Table 17](#) 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.
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.
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 in privileged EXEC mode.

show ip mobile router registration

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 new extensions in the registration request.
	12.2(15)T	This command was enhanced to display collocated care-of addresses (CCoAs) if configured.
	12.4(24)T	This command was enhanced to display link-type labels.

Examples The following is sample output from the **show ip mobile router registration** command:

```
MR# show ip mobile router registration

Mobile Router Registrations:

Foreign agent 192.0.2.112:
  Registration accepted 01/19/09 04:53:51, On Ethernet2/0
  Care-of addr 192.0.2.102, HA addr 192.0.2.3, Home addr 192.0.2.0
  Lifetime requested 00:01:30 (90), Granted 00:01:30 (90)
  Remaining 00:01:24
  Flags sbDmg-T-, Identification CD1E85DF.3D702EC8
  Register next time 00:00:39
  Extensions:
    Mobile Network 192.0.2.6/24
    MN-HA Authentication SPI 100

Home agent 192.0.2.3:
  Registration accepted 01/19/09 04:53:52, On Ethernet0/0
  Collocated care-of addr 192.0.2.103, HA addr 192.0.2.3, Home addr 192.0.2.0
  Lifetime requested 00:01:30 (90), Granted 00:01:30 (90)
  Remaining 00:01:25
  Flags sbDmg-T-, Identification CD1E85E0.3F7C7758
  Register next time 00:00:40
  Extensions:

Mobile Router Registrations:

  Mobile Network 192.0.2.6/24
  MN-HA Authentication SPI 100
```

```

Foreign agent 192.0.2.16:
  Registration accepted 01/19/09 04:53:51, On Ethernet1/0
  Care-of addr 192.0.2.104, HA addr 192.0.2.3, Home addr 192.0.2.0
  Lifetime requested 00:01:30 (90), Granted 00:01:30 (90)
  Remaining 00:01:23
  Flags sbdmg-T-, Identification CD1E85DF.3D702EC8
  Register next time 00:00:38
  Extensions:
    Mobile Network 192.0.2.6/24
    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 192.0.2.23:
  Registration accepted 01/01/02 10:24:46, On Ethernet5/3
  Collocated care-of addr 192.0.2.27, HA addr 192.0.2.23, Home addr 192.0.2.40
  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 192.0.2.4/24
    MN-HA Authentication SPI 100

```

[Table 18](#) 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.

Table 18 *show ip mobile router registration Field Descriptions (continued)*

Field	Description
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.
---------------------	---

Defaults

Displays counters since the counters were last cleared.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(24)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
```

Table 19 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.
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.

Table 19 *show ip mobile router traffic Field Descriptions (continued)*

Field	Description
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.
<i>ip-address</i>		IP address.
<i>nai string</i>		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
```

[Table 20](#) 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

```

Table 21 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).
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).

Table 21 *show ip mobile traffic Field Descriptions (continued)*

Field	Description
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).
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).

Table 21 *show ip mobile traffic Field Descriptions (continued)*

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).
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** command in EXEC mode.

```
show ip mobile tunnel [interface-type] [interface number]
```

Syntax Description

<i>interface-type</i>	(Optional) Displays a particular tunnel interface type. The <i>interface</i> argument is tunnel <i>x</i> .
<i>interface number</i>	(Optional) Displays a particular tunnel interface number. The <i>interface</i> argument is tunnel <i>x</i> .

Command Modes

Privileged 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.
12.4(24)T	This command was enhanced to display link-type labels.

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:

Total mobile ip tunnels 3
Tunnel2:
  src 192.0.2.103, dest 192.0.2.3, key 0
  encaps IP/IP, mode reverse-allowed, tunnel-users 1
  Input ACL users 0, Output ACL users 0
  IP MTU 1480 bytes
  Path MTU Discovery, mtu: 0, ager: 10 mins, expires: never
  outbound interface Ethernet0/0, link type WIFI
  MR created, CEF switching enabled, ICMP unreachable enabled
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
  0 packets input, 0 bytes, 0 drops
  0 packets output, 0 bytes
Tunnel1:
```

```

src 192.0.2.0, dest 192.0.2.3, key 7
encap IP/IP, mode reverse-allowed, tunnel-users 1
Input ACL users 0, Output ACL users 0
IP MTU 1480 bytes
Path MTU Discovery, mtu: 0, ager: 10 mins, expires: never
outbound interface Ethernet1/0, link type UMTS
MR created, CEF switching enabled, ICMP unreachable enabled Mobile Tunnels:

5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
0 packets input, 0 bytes, 0 drops
0 packets output, 0 bytes
Tunnel0:
src 192.0.2.0, dest 192.0.2.3, key 11
encap IP/IP, mode reverse-allowed, tunnel-users 1
Input ACL users 0, Output ACL users 0
IP MTU 1480 bytes
Path MTU Discovery, mtu: 0, ager: 10 mins, expires: never
outbound interface Ethernet2/0
MR created, CEF switching enabled, ICMP unreachable enabled
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
0 packets input, 0 bytes, 0 drops
0 packets output, 0 bytes

```

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 192.0.2.91, dest 192.0.2.97
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 192.0.2.100, dest 192.0.2.115
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 192.0.2.100, dest 192.0.2.207
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 192.0.2.97, dest 192.0.2.158
  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 192.0.2.172, dest 192.0.2.202 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

```

Table 22 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.

Table 22 *show ip mobile tunnel Field Descriptions (continued)*

Field	Description
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.
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)
```

[Table 23](#) 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.

Table 23 *show ip mobile violation Field Descriptions (continued)*

Field	Description
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: <ul style="list-style-type: none">• (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 in privileged EXEC mode.

```
show ip mobile visitor [[pending] [ip-address | summary] | nai string [session-id string]]
```

Syntax Description

pending	(Optional) Displays the pending registration table.
<i>ip-address</i>	(Optional) IP address of visiting MNs.
summary	(Optional) Displays all values in the table.
<i>nai string</i>	(Optional) Network access identifier (NAI).
session-id <i>string</i>	(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
```

Table 24 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.
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.

Table 24 *show ip mobile visitor Field Descriptions (continued)*

Field	Description
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.
Routing Options	Routing options list all foreign agent-accepted services, based on registration flags sent by the mobile node. Options are: <ul style="list-style-type: none"> • (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 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 mag binding

To display the list of the bindings established over the Proxy Mobile IPv6 (PMIP) signaling plane, use the **show ipv6 mobile pmipv6 mag binding** command in privileged EXEC mode.

```
show ipv6 mobile pmipv6 mag binding [lma lma-identifier | nai string]
```

Syntax Description

lma lma-identifier	(Optional) Displays the bindings for the Local Mobility Anchor (LMA).
nai string	(Optional) Displays the bindings for the mobile node (MN).

Command Default

The default syntax **show ipv6 mobile pmipv6 mag binding** displays the bindings established over the PMIP signaling plane.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

The **show ipv6 mobile pmipv6 mag binding lma lma-identifier** command displays the bindings established over the PMIP signaling plane for the LMA.

The **show ipv6 mobile pmipv6 mag binding nai string** command displays the bindings established over the PMIP signaling plane for the MN.

Examples

The following is sample output from the **show ipv6 mobile pmipv6 mag binding** command. The fields in the display are self-explanatory.

```
Router# show ipv6 mobile pmipv6 mag 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 lma-identifier** command. The fields in the display are self-explanatory.

```
Router# show ipv6 mobile pmipv6 mag binding lma lma1
```

```
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
-----
```

```
Router# show ipv6 mobile pmipv6 mag binding lma lma2
```

```
Total number of bindings: 1
```

```
-----
[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
-----
```

Related Commands

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

Syntax Description This command has no arguments or keywords.

Command Default The **show ipv6 mobile pmipv6 mag globals** command displays the 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.

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 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 PMIP domain.

show ipv6 mobile pmipv6 mag stats

To display the global Mobile Access Gateway (MAG) statistics, use the **show ipv6 mobile pmipv6 mag stats** command in privileged EXEC mode.

```
show ipv6 mobile pmipv6 mag stats [domain domain-name peer peer-name]
```

Syntax Description

domain <i>domain-name</i>	(Optional) Specifies the Proxy Mobile IPv6 (PMIP) domain.
peer <i>peer-name</i>	(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.

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:

```
Router# show ipv6 mobile pmipv6 mag 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
```

[Table 1](#) describes the significant fields shown in the display. The other fields are self-explanatory.

Table 25 *show ipv6 mobile pmipv6 mag stats* Field Descriptions

Field	Description
PBU Sent	The Proxy Binding Update sent from the MAG to the LMA.
PBA Rcvd	The Proxy Binding Acknowledgment received by the MAG.
PBRI Sent	The Proxy Binding Revocation Indication message sent from the LMA to the MAG and vice versa.

Table 25 show ipv6 mobile pmipv6 mag stats Field Descriptions (continued)

Field	Description
PBRI Rcvd	The Proxy Binding Revocation Indication message received by the LMA from the MAG and vice versa.
PBRA Sent	The Proxy Binding Revocation Acknowledgment message sent from the MAG to the LMA and vice versa.
PBRA Rcvd	The Proxy Binding Revocation Acknowledgment message 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 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 PMIP domain.
show interfaces tunnel 0 stats	Displays the PMIP 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]
```

Syntax Description		
	<i>process-id</i>	(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.
	<i>area-id</i>	(Optional) Displays information about a specified area only.

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
	12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Examples

show ipv6 ospf Output Example

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

```
Router# 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 msec
  Retransmission pacing timer 66 msec
  Number of external LSA 0. Checksum Sum 0x000000
  Number of areas in this router 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

```

Table 26 describes the significant fields shown in the display.

Table 26 *show ipv6 ospf Field Descriptions*

Field	Description
Routing process "ospfv3 1" with ID 10.10.10.1	Process ID and OSPF router ID.
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 router, area addresses, and so on.

show ipv6 ospf With Area Encryption Example

The following sample output shows the **show ipv6 ospf** command with area encryption information:

```

Router# show ipv6 ospf

Routing Process "ospfv3 1" with ID 10.0.0.1
It is an area border router
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 msec
Retransmission pacing timer 66 msec
Number of external LSA 0. Checksum Sum 0x000000
Number of areas in this router 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

```

Table 27 describes the significant fields shown in the display.

Table 27 *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).

show ipv6 ospf interface

To display Open Shortest Path First (OSPF)-related interface information, use the **show ipv6 ospf interface** command in user EXEC or privileged mode.

```
show ipv6 ospf [process-id] [area-id] interface [interface-type interface-number] [brief]
```

Syntax Description		
<i>process-id</i>	(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.
<i>area-id</i>	(Optional)	Displays information about a specified area only.
<i>interface-type</i> <i>interface-number</i>	(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.
	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.

Examples

show ipv6 ospf interface Standard Output Example

The following is sample output from the **show ipv6 ospf interface** 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
```

show ipv6 ospf interface

```

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)

```

Table 28 describes the significant fields shown in the display.

Table 28 *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.

Cisco IOS Release 12.2(33)SRB Example

The following is sample output of the **show ipv6 ospf interface** 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	

OSPF with Authentication on the Interface Example

The following is sample output from the **show ipv6 ospf interface** 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)
```

OSPF with Null Authentication Example

The following is sample output from the **show ipv6 ospf interface** 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)
```

OSPF with Authentication for the Area Example

The following is sample output from the **show ipv6 ospf interface** 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)
```

OSPF with Dynamic Cost Example

The following display shows sample output from the **show ipv6 ospf interface** command when the OSPF cost dynamic is configured.

```
Router1# show ipv6 ospf interface serial12/0

Serial12/0 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)
```

Related Commands

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

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
```

Interface	IPV6 Address	IPV4 Address	Uptime	Transmit Packets	Receive Packets
vmi1	::	10.3.3.2	00:02:11	0000000008	0000000073

[Table 29](#) describes the significant fields shown in the **show vmi neighbors** command display.

Table 29 *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.

show vmi neighbors command with detail keyword: Example

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
PADG xmit: 24 rcvd: 24
PADQ xmit: 0 rcvd: 0
```

[Table 30](#) describes the significant fields shown in the **show vmi neighbors detail** command display.

Table 30 *show vmi neighbors detail 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.

Table 30 show vmi neighbors detail Field Descriptions (continued)

Field	Description
Output pkts	Number of outgoing packets during the recorded up time.
Input pkts	Number of incoming packets during the recorded up time.
Metric Data	<p>The Metric data statistics</p> <p>Total rcvd: The total number of packets received on the interface</p> <p>Avg arrival rate: The average arrival rate for each packet in milliseconds.</p> <p>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</p> <p>MDR: The maximum, minimum, and average metric data rate</p> <p>CDR: The maximum, minimum, and average credit data rate</p> <p>Latency: The maximum, minimum, and average latency</p> <p>Resource: The maximum, minimum, and average resource</p> <p>RQL: The maximum, minimum, and average RQL</p> <p>Load: The maximum, minimum, and average load</p>
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.
PPPoE Flow Control Stats	<p>The statistics collected for PPPoE credit flow.</p> <p>Local Credits: The number of credits belonging to this node.</p> <p>Peer Credits: The number of credits belonging to the peer.</p> <p>Scalar Value: The credit grant in bytes specified by the radio</p> <p>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.</p> <p>Credit Starved Packets: The number of packets dropped or queued due to insufficient credits from the peer.</p> <p>Max Credits per grant: 65534</p> <p>PADG Seq Num: The sequence number for the PPPoE packet discovery grant</p> <p>PADG Timer index: The timer index for the PPPoE packet discovery grant</p> <p>PADG last rcvd Seq Num: The sequence number for the previously received PPPoE packet discovery grant</p> <p>PADG last nonzero Seq Num: The sequence number for the last non-zero PPPoE packet discovery grant</p> <p>PADG last nonzero rcvd amount: The received amount in the last non-zero PPPoE packet discovery grant</p> <p>PADG Timers: The PPPoE packet discovery grant timers</p> <p>PADG xmit: numeric rcvd: The number of PPPoE packet discovery grants transmitted and received</p> <p>PADC xmit: 133 rcvd: 133: The number of PPPoE packet discovery grant confirmations transmitted and received</p> <p>PADQ xmit: 0 rcvd: The number of PPPoE packet discovery quality grants transmitted and received.</p>

■ show vmi neighbors

Related Commands

Command	Description
debug vmi	Displays debugging output for VMIs.
interface vmi	Creates a VMI that can be configured and applied dynamically.

snmp-server enable traps ipmobile

To enable Simple Network Management Protocol (SNMP) security notifications for Mobile IP, use the **snmp-server enable traps ipmobile** command in 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.

Defaults

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.
snmp-server trap-source	Specifies the interface from which an SNMP trap should originate.

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	<i>interface-number</i>	Tunnel interface number.
---------------------------	-------------------------	--------------------------

Defaults	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	<i>interface-number</i>	Tunnel interface number.
--------------------	-------------------------	--------------------------

Defaults	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.

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 in mobile 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.

Defaults 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.