ip mobile host

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

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

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

Syntax Description

lower [*upper*]	One or a range of mobile host or mobile node group IP addresses. The upper end of the range is optional.
nai *string*	Network access identifier. The NAI can be a unique identifier (username@realm) or a group identifier (@realm).
static-address	(Optional) Indicates that a static IP address is to be assigned to the flows on this NAI. This parameter is not valid if the NAI is a realm.
addr1, addr2, ...	(Optional) One to a maximum of five IP addresses to be assigned using the **static-address** keyword.
local-pool *name*	(Optional) Name of the local pool of addresses to use for assigning a static IP address to this NAI.
address	(Optional) Indicates that a dynamic IP address is to be assigned to the flows on this NAI.
addr	(Optional) IP address to be assigned using the **address** keyword.
pool	(Optional) Indicates that a pool of addresses is to be used in assigning a dynamic IP address.
local *name*	(Optional) The name of the local pool to use in assigning addresses.
dhcp-proxy-client	(Optional) Indicates that the DHCP request should be sent to a DHCP server on behalf of the mobile node.
dhcp-server *addr*	(Optional) IP address of the DHCP server.
interface *name*	When used with DHCP, specifies the gateway address from which the DHCP server should select the address.
virtual-network *network-address mask*	Indicates that the mobile station resides in the specified virtual network, which was created using the **ip mobile virtual-network** command.
aaa	(Optional) Retrieves security associations from a AAA (TACACS+ or RADIUS) server. Allows the home agent to download address configuration details from the AAA server.
load-sa	(Optional) Caches security associations after retrieval by loading the security association into RAM. See Table 8 for details on how security associations are cached for NAI hosts and non-NAI hosts.

permanent	(Optional) Caches security associations in memory after retrieval permanently. Use this optional keyword only for NAI hosts.
authorized-pool *name*	(Optional) Verifies the IP address assigned to the mobile node if it is within the pool specified by the *name* argument.
skip-aaa-reauthentication	(Optional) When configured, the home agent does not send an access request for authentication for mobile IP re-registration requests. When disabled, the home agent sends an access request for all Mobile IP registration requests.
care-of-access *access-list*	(Optional) Access list. This can be a named access list or standard access list. The range is from 1 to 99. Controls where mobile nodes roam—the acceptable care-of addresses.
lifetime *seconds*	(Optional) Lifetime (in seconds). The lifetime for each mobile node (group) can be set to override the global value. The range is from 3 to 65535 (infinite).

Defaults

No host is configured.

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

All hosts must have security associations for registration authentication. Mobile nodes can have more than one security association. The memory consumption calculations shown in Table 7 are based on the assumption of one security association per mobile node. Caching behavior of security associations differs between NAI and non-NAI hosts as described in Table 8.

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

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

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

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

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

Each method has advantages and disadvantages, which are described in Table 7.

Table 7 Methods for Storing Security Associations

Storage Method	Advantage	Disadvantage
On the router	• Security association is in router memory, resulting in fast lookup. • For home agents supporting fewer than 1500 mobile nodes, this provides optimum authentication performance and security (keys never leave router).	• NVRAM of router is limited, cannot store many security associations. Each security association configuration takes about 80 bytes. For 125 KB NVRAM, you can store about 1500 security associations on a home agent.
On the AAA server, retrieve security association each time registration comes in	• Central administration and storage of security association on AAA server. • If keys change constantly, administration is simplified to one server, latest keys always retrieved during registration. • Router memory (DRAM) is conserved. Router will need memory only to load in a security association, and then release the memory when done.	• Requires network to retrieve security association, slower than other storage methods, and dependent on network and server performance. • Multiple home agents that use one AAA server, which can become the bottleneck, can get slow response. • Key can be snooped if packets used to retrieve from AAA are not encrypted (for example, using RADIUS or unencrypted TACACS+ mode).

Table 7 Methods for Storing Security Associations (continued)

Storage Method	Advantage	Disadvantage
On the AAA server, retrieve and store security association	• AAA acts as an offload configuration server, security associations are loaded into router DRAM, which is more abundant (for example, 16 MB, 32 MB, 64 MB) when the first registration comes in. Each security association takes only about 50 bytes of DRAM, so 10,000 mobile nodes will use up 0.5 MB. • If keys remain fairly constant, once security associations are loaded, home agent authenticates as fast as when stored on the router. • Only security associations that are needed are loaded into router memory. Mobile nodes that never register will not waste memory.	• If keys change on the AAA server after the mobile node registered, then you need to use **clear ip mobile secure** command to clear and load in new security association from AAA, otherwise the security association of the router is stale.

The caching behavior of security associations for NAI hosts and non-NAI hosts is described in Table 8.

Table 8 Caching Behavior for Security Associations

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

Note On the Mobile Wireless Home Agent, the following conditions apply:

If the **aaa load-sa** option is configured, the Home Agent caches the SA locally on first registration. In this case the Home Agent will not invoke the RADIUS authorization procedure for re-registration.

If **aaa load-sa skip-aaa-reauthentication** is configured, the Home Agent caches the SA locally on first registration; however, the Home Agent will not invoke HA-CHAP procedure for re-registration.

The **aaa load-sa permanent** option is not supported on the Mobile Wireless Home Agent, and should not be configured.

Examples

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Related Commands

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

ip mobile radius disconnect

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

ip mobile radius disconnect

no ip mobile radius disconnect

Syntax Description

This command has no arguments or keywords.

Command Default

Radius Disconnect messages are not processed by the home agent.

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

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

Examples

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

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

ip mobile realm

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

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

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

Syntax Description

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

Defaults

There are no default values for this command.

Command Modes

Global configuration

Command History

Release	Modification
12.3(7)XJ.	This command was introduced.
12.3(14)YX	The dns server assign, and dns dynamic-update method variables were introduced.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.

Usage Guidelines

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

Examples

The following example identifies the DNS **dynamic update** keyword:

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

The following example identifies the **hotlining** and **vrf** keywords:

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

vrf VRF for the realm

ip mobile secure

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

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

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

Syntax Description

aaa-download	Downloads security association from AAA at every timer interval.
host	Security association of the mobile host on the home agent.
visitor	Security association of the mobile host on the foreign agent.
home-agent	Security association of the remote home agent on the foreign agent.
foreign-agent	Security association of the remote foreign agent on the home agent.
proxy-host	Security association of the proxy Mobile IP users. This keyword is only available on Packet Data Serving Node (PDSN) platforms.
lower-address	IP address of a host or lower range of IP address pool.
upper-address	(Optional) Upper range of an IP address pool. If specified, security associations for multiple hosts are configured. The value used in the *upper-address* argument must be greater than that used in the *lower-address* argument.
nai *string*	Network access identifier of the mobile node. The **nai** *string* is valid only for a host, visitor, and proxy host.
inbound-spi *spi-in*	Security parameter index used for authenticating inbound registration packets. Range is from 0x100 to 0xffffffff.
outbound-spi *spi-out*	Security parameter index used for calculating the authenticator in outbound registration packets. Range is from 0x100 to 0xffffffff.
spi *spi*	Bidirectional SPI. Range is from 0x100 to 0xffffffff.
key hex *string*	ASCII string of hexadecimal values. No spaces are allowed.
replay	(Optional) Specifies replay protection used on registration packets.
timestamp	(Optional) Validates incoming packets to ensure that they are not being “replayed” by a spoofer using the timestamp method.
number	(Optional) Number of seconds. Registration is valid if received within the router’s clock +/- 7 seconds. This means the sender and receiver are in time synchronization (NTP can be used).
algorithm	(Optional) Algorithm used to authenticate messages during registration.
md5	(Optional) Message Digest 5.
hmac-md5	(Optional) Hash-based message authentication code (HMAC) message digest 5.

mode	(Optional) Mode used to authenticate during registration.
prefix-suffix	(Optional) The key is used to wrap the registration information for authentication (for example, key registration information key) to calculate the message digest.

Defaults

No security association is specified.

Command Modes

Global configuration

Command History

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

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

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

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

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

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

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

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

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

Examples

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

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

Related Commands

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

ip mobile tunnel

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

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

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

Syntax Descriptionl

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

Defaults

Disabled.

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

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

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

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

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

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

Examples

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

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

Related Commands

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

ip mobile virtual-network

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

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

no ip mobile virtual-network *net mask*

Syntax Description

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

Defaults

No home agent addresses are specified.

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

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

Examples

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

```
interface ethernet 0
 ip address 1.0.0.1 255.0.0.0
 standby ip 1.0.0.10
 standby name SanJoseHA

interface loopback 0
 ip address 20.0.0.1 255.255.255.255

ip mobile home-agent
 ip mobile virtual-network 20.0.0.0 255.255.0.0 address 20.0.0.1
 ip mobile home-agent standby SanJoseHA virtual-network
 ip mobile secure home-agent 1.0.0.2 spi 100 hex 00112233445566778899001122334455
```

Related Commands

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

radius-server attribute 32 include-in-access-req

To send RADIUS attribute 32 (NAS-Identifier) in an access-request or accounting-request, use the **radius-server attribute 32 include-in-access-req** command in global configuration mode. To disable sending RADIUS attribute 32, use the **no** form of this command.

radius-server attribute 32 include-in-access-req [*format*]

no radius-server attribute 32 include-in-access-req

Syntax Description

format	(Optional) A string sent in attribute 32 containing an IP address (%i), a hostname (%h), or a domain name (%d).

Defaults

RADIUS attribute 32 is not sent in access-request or accounting-request packets.

Command Modes

Global configuration

Command History

Release	Modification
12.1 T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Using the **radius-server attribute 32 include-in-access-req** command makes it possible to identify the network access server (NAS) manufacturer to the RADIUS server by sending RADIUS attribute 32 (NAS-Identifier) in an access-request or accounting-request. If you configure the format argument, the string sent in attribute 32 will include an IP address, a hostname, or a domain name; otherwise, the Fully Qualified Domain Name (FQDN) is sent by default.

Examples

The following example shows a configuration that sends RADIUS attribute 32 in the access-request with the format configured to identify a Cisco NAS:

```
radius-server attribute 32 include-in-access-req format cisco %h.%d %i
! The following string will be sent in attribute 32 (NAS-Identifier).
"cisco router.nlab.cisco.com 10.0.1.67"
```

radius-server host

To specify a RADIUS server host, use the **radius-server host** command in global configuration mode. To delete the specified RADIUS host, use the **no** form of this command.

radius-server host {*hostname* | *ip-address*} [**test username** *user-name*] [**auth-port** *port-number*]
[**ignore-auth-port**] [**acct-port** *port-number*] [**ignore-acct-port**] [**timeout** *seconds*]
[**retransmit** *retries*] [**key** *string*] [**alias** {*hostname* | *ip-address*}] [**idle-time** *seconds*]

no radius-server host {*hostname* | *ip-address*}

Syntax Description

hostname	Domain Name System (DNS) name of the RADIUS server host.
ip-address	IP address of the RADIUS server host.
test username	(Optional) Turns on the automated testing feature for RADIUS server load balancing.
user-name	(Optional) Test user ID username. • Must be used if the **test username** keyword is used. **Caution** It is recommended that a test user, one that is not defined on the RADIUS server, be used for RADIUS server automated testing to protect against security issues that may arise if the test user is not correctly configured.
auth-port	(Optional) Specifies the UDP destination port for authentication requests.
port-number	(Optional) Port number for authentication requests; the host is not used for authentication if set to 0. If unspecified, the port number defaults to 1645.
ignore-auth-port	(Optional) Turns off the automated testing feature for RADIUS server load balancing on the authentication port.
acct-port	(Optional) Specifies the UDP destination port for accounting requests.
port-number	(Optional) Port number for accounting requests; the host is not used for accounting if set to 0. If unspecified, the port number defaults to 1646.
ignore-acct-port	(Optional) Turns off the automated testing feature for RADIUS server load balancing on the accounting port.
timeout	(Optional) The time interval (in seconds) that the router waits for the RADIUS server to reply before retransmitting. This setting overrides the global value of the **radius-server timeout** command. If no timeout value is specified, the global value is used. Enter a value in the range 1 to 1000.
seconds	(Optional) Specifies the **timeout** value. Enter a value in the range 1 to 1000. If no **timeout** value is specified, the global value is used.
retransmit	(Optional) The number of times a RADIUS request is re-sent to a server, if that server is not responding or responding slowly. This setting overrides the global setting of the **radius-server retransmit** command.
retries	(Optional) Specifies the retransmit value. Enter a value in the range 1 to 100. If no retransmit value is specified, the global value is used.

key	(Optional) Specifies the authentication and encryption key used between the router and the RADIUS daemon running on this RADIUS server. This key overrides the global setting of the **radius-server key** command. If no key string is specified, the global value is used. The key is a text string that must match the encryption key used on the RADIUS server. Always configure the key as the last item in the **radius-server host** command syntax. This is because the leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in the key, do not enclose the key in quotation marks unless the quotation marks themselves are part of the key.
string	(Optional) Specifies the authentication and encryption key for all RADIUS communications between the router and the RADIUS server. This key must match the encryption used on the RADIUS daemon. All leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in your key, do not enclose the key in quotation marks unless the quotation marks themselves are part of the key.
alias	(Optional) Allows up to eight aliases per line for any given RADIUS server.
idle-time	(Optional) Specifies the time the server remains idle before it is quarantined and test packets are sent out.
seconds	(Optional) Length of idle time. • Default is 3600 seconds (1 hour). The valid range is 1–35791 seconds.

Defaults

No RADIUS host is specified; use global **radius-server** command values.

RADIUS server load balancing automated testing is disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.
12.0(5)T	This command was modified to add options for configuring timeout, retransmission, and key values per RADIUS server.
12.1(3)T	The **alias** keyword was added on the Cisco AS5300 and AS5800 universal access servers.
12.2(28)SB	The following keywords and arguments were added for configuring RADIUS server load balancing automated testing functionality: **test username** *user-name*, **ignore-auth-port**, **ignore-acct-port**, and **idle-time** *seconds*.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

You can use multiple **radius-server host** commands to specify multiple hosts. The software searches for hosts in the order in which you specify them.

If no host-specific timeout, retransmit, or key values are specified, the global values apply to each host.

RADIUS Server Automated Testing

When using the **radius-server host** command to enable automated testing for RADIUS server load balancing:

The authentication port is checked by default. If not specified, the default port of 1645 is used. If you wish to not check the authentication port, the **ignore-auth-port** keyword must be specified.

The accounting port is checked by default. If not specified, the default port of 1645 is used. If you wish to not check the accounting port, the **ignore-acct-port** keyword must be specified.

Examples

The following example specifies *host1* as the RADIUS server and uses default ports for both accounting and authentication:

```
radius-server host host1
```

The following example specifies port 1612 as the destination port for authentication requests and port 1616 as the destination port for accounting requests on the RADIUS host named host1:

```
radius-server host host1 auth-port 1612 acct-port 1616
```

Because entering a line resets all the port numbers, you must specify a host and configure accounting and authentication ports on a single line.

The following example specifies the host with IP address 192.0.2.46 as the RADIUS server, uses ports 1612 and 1616 as the authorization and accounting ports, sets the timeout value to 6, sets the retransmit value to 5, and sets “rad123” as the encryption key, matching the key on the RADIUS server:

```
radius-server host 192.0.2.46 auth-port 1612 acct-port 1616 timeout 6 retransmit 5 key
rad123
```

To use separate servers for accounting and authentication, use the zero port value as appropriate.

The following example specifies that RADIUS server host1 be used for accounting but not for authentication, and that RADIUS server host2 be used for authentication but not for accounting:

```
radius-server host host1.example.com auth-port 0
radius-server host host2.example.com acct-port 0
```

The following example specifies four aliases on the RADIUS server with IP address 192.0.2.1:

```
radius-server host 192.0.2.1 acct-port 1645 auth-port 1646
radius-server host 192.0.2.1 alias 192.0.2.2 192.0.2.3 192.0.2.4
```

The following example shows how to enable RADIUS server automated testing for load balancing with the authorization and accounting ports specified:

```
radius-server host 192.0.2.176 test username test1 auth-port 1645 acct-port 1646
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes.
aaa authentication ppp	Specifies one or more AAA authentication method for use on serial interfaces running PPP.
aaa authorization	Sets parameters that restrict network access to a user.
debug aaa test	Shows when the idle-timer or dead-timer has expired for RADIUS server load balancing.
load-balance	Enables RADIUS server load balancing for named RADIUS server groups.
ppp	Starts an asynchronous connection using PPP.
ppp authentication	Enables CHAP or PAP or both and specifies the order in which CHAP and PAP authentication are selected on the interface.
radius-server key	Sets the authentication and encryption key for all RADIUS communications between the router and the RADIUS daemon.
radius-server load-balance	Enables RADIUS server load balancing for the global RADIUS server group.
radius-server retransmit	Specifies how many times the Cisco IOS software searches the list of RADIUS server hosts before giving up.
radius-server timeout	Sets the interval a router waits for a server host to reply.
test aaa group	Tests RADIUS load balancing server response manually.
username	Establishes a username-based authentication system, such as PPP CHAP and PAP.

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.

show ip mobile binding

To display the mobility binding table on the home agent (HA), use the **show ip mobile binding** command in privileged EXEC mode.

show ip mobile binding [**home-agent** *ip-address* | **nai** *string* [**session-id** *string*] | **summary**]

Syntax Description

home-agent	(Optional) Mobility bindings for a specific home agent (HA).
ip-address	(Optional) IP address for the HA.
nai *string*	(Optional) Mobile node (MN) identified by the network access identifier (NAI).
session-id *string*	(Optional) Session identifier. The *string* argument must be fewer than 25 characters in length.
summary	(Optional) Total number of bindings in the table.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.0(2)T	The **home-agent** keyword and *ip-address* argument were added.
12.1(2)T	The **summary** keyword was added.
12.2(2)XC	The **nai** keyword was added.
12.2(13)T	This command was enhanced to display the service options field and to include information about the mobile networks registered on the home agent.
12.3(4)T	The **session-id** keyword was added.
12.3(8)T	The output was enhanced to display UDP tunneling information.
12.4(9)T	The output was enhanced to display multipath support.

Usage Guidelines

You can display a list of all bindings if you press enter. You can also specify an IP address for a specific home agent using the **show ip mobile binding home-agent** *ip-address* command.

If the **session-id** *string* combination is specified, only the binding entry for that session identifier is displayed. A session identifier is used to uniquely identify a Mobile IP flow. A Mobile IP flow is the set of {NAI, IP address}. The flow allows a single NAI to be associated with one or multiple IP addresses, for example, {NAI, ipaddr1}, {NAI, ipaddr2}, and so on. A single user can have multiple sessions for example, when logging through different devices such as a PDA, cellular phone, or laptop. If the session identifier is present in the initial registration, it must be present in all subsequent registration renewals from that MN.

Examples

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

```
Router# show ip mobile binding

Mobility Binding List:
```

```
Total 1
10.0.0.1:
 Care-of Addr 10.0.0.31, Src Addr 10.0.0.31,
 Lifetime granted 02:46:40 (10000), remaining 02:46:32
 Flags SbdmGvt, Identification B750FAC4.C28F56A8,
 Tunnel100 src 10.0.0.5 dest 10.0.0.31 reverse-allowed
 Routing Options - (G)GRE
  Service Options:
  NAT detect
```

The following is sample output from the **show ip mobile binding** command when mobile networks are configured or registered on the home agent:

```
Router# show ip mobile binding

Mobility Binding List:
Total 1
10.0.4.1:
 Care-of Addr 10.0.0.5, Src Addr 10.0.0.5
 Lifetime granted 00:02:00 (120), remaining 00:01:56
 Flags sbDmgvT, Identification B7A262C5.DE43E6F4
 Tunnel0 src 10.0.0.3 dest 10.0.0.5 reverse-allowed
 MR Tunnel1 src 10.0.0.3 dest 10.0.4.1 reverse-allowed
 Routing Options - (D)Direct-to-MN (T)Reverse-tunnel
 Mobile Networks: 10.0.0.0/255.255.255.0(S)
  10.0.0.0/255.255.255.0 (D)
  10.0.0.0/255.0.0.0(D)
```

The following is sample output from the **show ip mobile binding** command with session identifier information:

```
Router# show ip mobile binding

Mobility Binding List:
Total 1
 10.100.100.19:
 Care-of Addr 10.70.70.2, Src Addr 10.100.100.1,
 Lifetime granted 00:33:20 (20000), remaining 00:30:56
 Flags SbdmGvt, Identification BC1C2A04.EA42659C,
 Tunnel0 src 10.100.100.100 dest 10.70.70.2 reverse-allowed
 Routing Options
 Session identifier 998811234
 SPI 333 (decimal 819) MD5, Prefix-suffix, Timestamp +/-255, root key
 Key 38a38987ad0a399cb80940835689da66
 SPI 334 (decimal 820) MD5, Prefix-suffix, Timestamp +/-255, session key
 Key 34c7635a313038611dec8c16681b55e0
```

The following sample output shows that the home agent is configured to detect network address translation (NAT):

```
Router# show ip mobile binding nai mn@cisco.com

Mobility Binding List:

 mn@cisco.com (Bindings 1):
 Home Addr 10.99.101.1
 Care-of Addr 192.168.1.202, Src Addr 192.168.157.1
 Lifetime granted 00:03:00 (180), remaining 00:02:20
 Flags sbDmg-T-, Identification BCF5F7FF.92C1006F
 Tunnel0 src 192.168.202.1 dest 192.168.157.1 reverse-allowed
 Routing Options - (D)Direct-to-MN (T)Reverse-tunnel
 Service Options:
 NAT detect
```

The following sample output shows that multipath support is enabled:

```
Router# show ip mobile binding

Mobility Binding List:
Total 1
10.1.1.1:
    Care-of Addr 10.1.1.11, Src Addr 10.1.1.11
    Lifetime granted 10:00:00 (36000), remaining 09:52:40
    Flags sbDmg-T-, Identification C5441314.61D36B14
    Tunnel1 src 12.1.1.10 dest 10.1.1.11 reverse-allowed
    MR Tunnel1 src 12.1.1.10 dest 10.1.1.11 reverse-allowed
    Routing Options - (D)Direct-to-MN (T)Reverse-tunnel
    Mobile Networks: 10.38.0.0/255.255.0.0 (D)
    Roaming IF Attributes: BW 10000 Kbit, ID 3247
     Description First Lan Interface
    Multi-path Metric bandwidth
```

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.
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.

Table 9 show ip mobile binding Field Descriptions (continued)

Field	Description
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.
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 binding

To display the mobility binding table, use the **show ip mobile binding** EXEC command.

show ip mobile binding [ip address | **home-agent** *address* | ***nai*** *string* | **summary** | **vrf [realm** ***vrf-realm*****]** **[summary]**]

Syntax Description

ip address	IP address of the Home agent
home-agent *address*	(Optional) IP address of mobile node.
nai string	(Optional) Network access identifier.
summary	(Optional) Displays the total number of bindings that are VRF-enabled.
vrf	(Optional) VRF of the user.
realm	(Optional) Displays the vrf realm.

Command Modes

EXEC

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.0(2)T	The following keyword and argument were added: • **home-agent** *address*
12.1(2)T	The **summary** keyword was added.
12.2(2)XC	The **nai** keyword was added.
12.3(7)XJ	This command was modified to display VRF related info if the realm of the NAI is under a VRF.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.

Usage Guidelines

The Home Agent updates the mobility binding table in response to registration events from mobile nodes. If the *address* argument is specified, bindings are shown for only that mobile node.

Examples

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

```
Router# show ip mobile binding

Mobility Binding List:
Total 1
mwts-mip-r20sit-haslb@ispxyz.com (Bindings 1):
    Home Addr 40.0.0.2
    Care-of Addr 20.20.210.10, Src Addr 20.20.210.10
    Lifetime granted 00:05:00 (300), remaining 00:04:11
    Flags sBdmg-T-, Identification C70D0890.10000
    Tunnel0 src 20.20.202.102 dest 20.20.210.10 reverse-allowed
    Tunnel0 Input ACL: mipinacl
    Tunnel0 Output ACL: mipoutacl
    Routing Options - (B)Broadcast (T)Reverse-tunnel
    Service Options:
        Dynamic HA assignment
    Revocation negotiated - I-bit set
    Acct-Session-Id: 43
    Sent on tunnel to MN: 0 packets, 0 bytes
    Received on reverse tunnel from MN: 0 packets, 0 bytes
    Radius Disconnect Enabled
    DNS Address primary 10.77.155.10 secondary 6.6.6.6
    DNS Address Assignment enabled with entity Configured at Homeagent(3)
    Dynamic DNS update to server enabled
ha2#
```

If the DNS server configs configured locally are used then the show output will include the following:

```
router# show ip mobile binding
Mobility Binding List:
    Total 1
    mwts-mip-r20sit-haslb@ispxyz20.com (Bindings 1):
    Home Addr 40.0.0.2
    Care-of Addr 20.20.210.10, Src Addr 20.20.210.10
    Lifetime granted 00:03:00 (180), remaining 00:02:32
    Flags sBdmg-T-, Identification C6ACD1D7.10000
    Tunnel0 src 20.20.202.102 dest 20.20.210.10 reverse-allowed
    Routing Options - (B)Broadcast (T)Reverse-tunnel
    Service Options:
    Dynamic HA assignment
    Revocation negotiated - I-bit set
    Acct-Session-Id: 23
    Sent on tunnel to MN: 0 packets, 0 bytes
    Received on reverse tunnel from MN: 0 packets, 0 bytes
    DNS Address primary 10.77.155.10 secondary 5.5.5.5
    DNS Address Assignment enabled with entity Configured at Homeagent(3)
```

If the DNS server addresses downloaded using a DNS server VSA from HAAA, then the show output will include the following:

```
router# show ip mobile binding
Mobility Binding List:
    Total 1
    mwts-mip-r20sit-haslb@ispxyz30.com (Bindings 1):
    Home Addr 40.0.0.3
    Care-of Addr 20.20.210.10, Src Addr 20.20.210.10
    Lifetime granted 00:03:00 (180), remaining 00:02:05
    Flags sBdmg-T-, Identification C6ACD910.10000
    Tunnel0 src 20.20.202.102 dest 20.20.210.10 reverse-allowed
    Routing Options - (B)Broadcast (T)Reverse-tunnel
    Service Options:
    Dynamic HA assignment
    Revocation negotiated - I-bit set
    Acct-Session-Id: 31
    Sent on tunnel to MN: 0 packets, 0 bytes
    Received on reverse tunnel from MN: 0 packets, 0 bytes
    DNS Address primary 10.77.155.10 secondary 10.77.155.9
    DNS Address Assignment enabled with entity From Home AAA(1)
```

Note If the DNS server address is configured both locally and downloaded from AAA, then preference will be given to the local configuration on the HA.

ACLs Applied to a Mobility Binding and Accounting Session ID and Accounting Counters

```
router# show ip mobile binding 44.0.0.1
Mobility Binding List:
    44.0.0.1:
    Care-of Addr 55.0.0.11, Src Addr 55.0.0.11
    Lifetime granted 00:01:30 (90), remaining 00:00:51
    Flags sbDmg-T-, Identification C661D5A0.4188908
    Tunnel1 src 46.0.0.3 dest 55.0.0.11 reverse-allowed
    Tunnel1 Input ACL: inaclname
    Tunnel1 Output ACL: outaclname - Empty list or not configured.
    MR Tunnel1 src 46.0.0.3 dest 55.0.0.11 reverse-allowed
    Routing Options - (D)Direct-to-MN (T)Reverse-tunnel
    Mobile Networks: 111.0.0.0/255.0.0.0 (S)
    Acct-Session-Id: 0
    Sent on tunnel to MN: 0 packets, 0 bytes
    Received on reverse tunnel from MN: 0 packets, 0 bytes

router# show ip mobile tunnel

Mobile Tunnels:
    Total mobile ip tunnels 1
    Tunnel0:
    src 46.0.0.3, dest 55.0.0.11
    encap IP/IP, mode reverse-allowed, tunnel-users 1
    Input ACL users 1, Output ACL users 1
    IP MTU 1480 bytes
    Path MTU Discovery, mtu: 0, ager: 10 mins, expires: never
    outbound interface Ethernet1/0
    HA created, fast 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 binding vrf summary** command:

```
router# show ip mobile binding vrf summary
Mobility Binding List:
Total number of VRF bindings is 1
```

If the VRF name downloaded from the HAAA and what is configured locally matches , then the **show ip mobile binding vrf realm** command will display the ouput below:

```
router# show ip mobile binding vrf realm @ispxyz1.com
Mobility Binding List:
Total bindings for realm @ispxyz1.com under VRF ispxyz-vrf1 is 1
mwts-mip-r20sit-has1b1@ispxyz1.com (Bindings 1):
Home Addr 50.0.0.2
Care-of Addr 20.20.210.10, Src Addr 20.20.210.10
Lifetime granted 00:05:00 (300), remaining 00:03:59
Flags sBdmg-T-, Identification C6DF047C.10000
Tunnel0 src 20.20.204.2 dest 20.20.210.10 reverse-allowed
Routing Options - (B)Broadcast (T)Reverse-tunnel
Service Options:
Dynamic HA assignment
Revocation negotiated - I-bit set
VRF ispxyz-vrf1
Acct-Session-Id: 17
Sent on tunnel to MN: 0 packets, 0 bytes
Received on reverse tunnel from MN: 0 packets, 0 bytes
Radius Disconnect Enabled
DNS Address primary 10.77.155.10 secondary 1.1.1.1
DNS Address Assignment enabled with entity Configured at Homeagent(3)
Dynamic DNS update to server enabled
```

If VRF is not configured locally, then the **show** output will be as below:

```
router# show ip mobile binding vrf realm @ispxyz1.com summary
Mobility Binding List:
```

%VRF is not enabled locally for realm @ispxyz1.com

Table 10 describes the significant fields shown in the display.

Table 10 show ip mobile binding Field Descriptions

Field	Description
Total	Total number of mobility bindings.
IP address	Home IP address of the mobile node.
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 collocated care-of address of a mobile node or an address of the Foreign Agent.
Lifetime granted	The lifetime granted to the mobile node for this registration. Number of seconds in parentheses.
Lifetime remaining	The time remaining until the registration is expired. It has the same initial value as lifetime granted, and is counted down by the Home Agent.
Flags	Registration flags sent by mobile node. 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 is IPIP encapsulation, otherwise GRE will be displayed in the Routing Options field.
Routing Options	Routing options list all Home Agent-accepted services. 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).

show ip mobile binding

To display the mobility binding table, use the **show ip mobile binding** EXEC command.

show ip mobile binding [ip address | **home-agent** *address* | ***nai*** *string* | **summary** | **vrf [realm** ***vrf-realm***] **[summary]**]

Syntax Description

ip address	IP address of the Home agent
home-agent *address*	(Optional) IP address of mobile node.
nai string	(Optional) Network access identifier.
summary	(Optional) Displays the total number of bindings that are VRF-enabled.
vrf	(Optional) VRF of the user.
realm	(Optional) Displays the vrf realm.

Command Modes

EXEC

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.0(2)T	The following keyword and argument were added: • **home-agent** *address*
12.1(2)T	The **summary** keyword was added.
12.2(2)XC	The **nai** keyword was added.
12.3(7)XJ	This command was modified to display VRF related info if the realm of the NAI is under a VRF.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.

Usage Guidelines

The Home Agent updates the mobility binding table in response to registration events from mobile nodes. If the *address* argument is specified, bindings are shown for only that mobile node.

Examples

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

```
Router# show ip mobile binding

Mobility Binding List:
Total 1
mwts-mip-r20sit-haslb@ispxyz.com (Bindings 1):
    Home Addr 40.0.0.2
    Care-of Addr 20.20.210.10, Src Addr 20.20.210.10
    Lifetime granted 00:05:00 (300), remaining 00:04:11
    Flags sBdmg-T-, Identification C70D0890.10000
    Tunnel0 src 20.20.202.102 dest 20.20.210.10 reverse-allowed
    Tunnel0 Input ACL: mipinacl
    Tunnel0 Output ACL: mipoutacl
    Routing Options - (B)Broadcast (T)Reverse-tunnel
    Service Options:
        Dynamic HA assignment
    Revocation negotiated - I-bit set
    Acct-Session-Id: 43
    Sent on tunnel to MN: 0 packets, 0 bytes
    Received on reverse tunnel from MN: 0 packets, 0 bytes
    Radius Disconnect Enabled
    DNS Address primary 10.77.155.10 secondary 6.6.6.6
    DNS Address Assignment enabled with entity Configured at Homeagent(3)
    Dynamic DNS update to server enabled
ha2#
```

If the DNS server configs configured locally are used then the show output will include the following:

```
router# show ip mobile binding
Mobility Binding List:
    Total 1
    mwts-mip-r20sit-haslb@ispxyz20.com (Bindings 1):
    Home Addr 40.0.0.2
    Care-of Addr 20.20.210.10, Src Addr 20.20.210.10
    Lifetime granted 00:03:00 (180), remaining 00:02:32
    Flags sBdmg-T-, Identification C6ACD1D7.10000
    Tunnel0 src 20.20.202.102 dest 20.20.210.10 reverse-allowed
    Routing Options - (B)Broadcast (T)Reverse-tunnel
    Service Options:
    Dynamic HA assignment
    Revocation negotiated - I-bit set
    Acct-Session-Id: 23
    Sent on tunnel to MN: 0 packets, 0 bytes
    Received on reverse tunnel from MN: 0 packets, 0 bytes
    DNS Address primary 10.77.155.10 secondary 5.5.5.5
    DNS Address Assignment enabled with entity Configured at Homeagent(3)
```

If the DNS server addresses downloaded using a DNS server VSA from HAAA, then the show output will include the following:

```
router# show ip mobile binding
Mobility Binding List:
    Total 1
    mwts-mip-r20sit-haslb@ispxyz30.com (Bindings 1):
    Home Addr 40.0.0.3
    Care-of Addr 20.20.210.10, Src Addr 20.20.210.10
    Lifetime granted 00:03:00 (180), remaining 00:02:05
    Flags sBdmg-T-, Identification C6ACD910.10000
    Tunnel0 src 20.20.202.102 dest 20.20.210.10 reverse-allowed
    Routing Options - (B)Broadcast (T)Reverse-tunnel
    Service Options:
    Dynamic HA assignment
    Revocation negotiated - I-bit set
    Acct-Session-Id: 31
    Sent on tunnel to MN: 0 packets, 0 bytes
    Received on reverse tunnel from MN: 0 packets, 0 bytes
    DNS Address primary 10.77.155.10 secondary 10.77.155.9
    DNS Address Assignment enabled with entity From Home AAA(1)
```

Note If the DNS server address is configured both locally and downloaded from AAA, then preference will be given to the local configuration on the HA.

ACLs Applied to a Mobility Binding and Accounting Session ID and Accounting Counters

```
router# show ip mobile binding 44.0.0.1
Mobility Binding List:
    44.0.0.1:
    Care-of Addr 55.0.0.11, Src Addr 55.0.0.11
    Lifetime granted 00:01:30 (90), remaining 00:00:51
    Flags sbDmg-T-, Identification C661D5A0.4188908
    Tunnel1 src 46.0.0.3 dest 55.0.0.11 reverse-allowed
    Tunnel1 Input ACL: inaclname
    Tunnel1 Output ACL: outaclname - Empty list or not configured.
    MR Tunnel1 src 46.0.0.3 dest 55.0.0.11 reverse-allowed
    Routing Options - (D)Direct-to-MN (T)Reverse-tunnel
    Mobile Networks: 111.0.0.0/255.0.0.0 (S)
    Acct-Session-Id: 0
    Sent on tunnel to MN: 0 packets, 0 bytes
    Received on reverse tunnel from MN: 0 packets, 0 bytes

router# show ip mobile tunnel

Mobile Tunnels:
    Total mobile ip tunnels 1
    Tunnel0:
    src 46.0.0.3, dest 55.0.0.11
    encap IP/IP, mode reverse-allowed, tunnel-users 1
    Input ACL users 1, Output ACL users 1
    IP MTU 1480 bytes
    Path MTU Discovery, mtu: 0, ager: 10 mins, expires: never
    outbound interface Ethernet1/0
    HA created, fast 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 binding vrf summary** command:

```
router# show ip mobile binding vrf summary
Mobility Binding List:
Total number of VRF bindings is 1
```

If the VRF name downloaded from the HAAA and what is configured locally matches , then the **show ip mobile binding vrf realm** command will display the ouput below:

```
router# show ip mobile binding vrf realm @ispxyz1.com
Mobility Binding List:
Total bindings for realm @ispxyz1.com under VRF ispxyz-vrf1 is 1
mwts-mip-r20sit-haslb1@ispxyz1.com (Bindings 1):
Home Addr 50.0.0.2
Care-of Addr 20.20.210.10, Src Addr 20.20.210.10
Lifetime granted 00:05:00 (300), remaining 00:03:59
Flags sBdmg-T-, Identification C6DF047C.10000
Tunnel0 src 20.20.204.2 dest 20.20.210.10 reverse-allowed
Routing Options - (B)Broadcast (T)Reverse-tunnel
Service Options:
Dynamic HA assignment
Revocation negotiated - I-bit set
VRF ispxyz-vrf1
Acct-Session-Id: 17
Sent on tunnel to MN: 0 packets, 0 bytes
Received on reverse tunnel from MN: 0 packets, 0 bytes
Radius Disconnect Enabled
DNS Address primary 10.77.155.10 secondary 1.1.1.1
DNS Address Assignment enabled with entity Configured at Homeagent(3)
Dynamic DNS update to server enabled
```

If VRF is not configured locally, then the **show** output will be as below:

```
router# show ip mobile binding vrf realm @ispxyz1.com summary
Mobility Binding List:
```

%VRF is not enabled locally for realm @ispxyz1.com

Table 11 describes the significant fields shown in the display.

Table 11 show ip mobile binding Field Descriptions

Field	Description
Total	Total number of mobility bindings.
IP address	Home IP address of the mobile node.
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 collocated care-of address of a mobile node or an address of the Foreign Agent.
Lifetime granted	The lifetime granted to the mobile node for this registration. Number of seconds in parentheses.
Lifetime remaining	The time remaining until the registration is expired. It has the same initial value as lifetime granted, and is counted down by the Home Agent.
Flags	Registration flags sent by mobile node. 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 is IPIP encapsulation, otherwise GRE will be displayed in the Routing Options field.
Routing Options	Routing options list all Home Agent-accepted services. 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).

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 12 describes the significant fields shown in the sample output.

Table 12 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 12 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 12 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** | **summary**]

Syntax Description

address	(Optional) IP address of specific mobile node. If not specified, information for all mobile nodes is displayed.
interface *interface*	(Optional) Displays all mobile nodes whose home network is on this interface.
network *address*	(Optional) Displays all mobile nodes residing on this network or virtual network.
nai *string*	(Optional) Network access identifier.
group	(Optional) Displays all mobile node groups configured using the **ip mobile host** command.
summary	(Optional) Displays all values in the table.

Command Modes

Privileged EXEC

Command History

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

Examples

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

```
Router# show ip mobile host

10.34.253.147:
   Allowed lifetime 10:00:00 (36000/default)
   Roam status -Registered-, Home link on virtual network 10.34.253.128 /26
   Accepted 2082, Last time 02/13/03 01:03:24
   Overall service time 1w0d
   Denied 32, Last time 01/03/03 21:13:43
   Last code 'registration id mismatch (133)'
   Total violations 32
   Tunnel to MN - pkts 0, bytes 0
   Reverse tunnel from MN - pkts 0, bytes 0
```

The following is sample output from the **show ip mobile host nai** *string* command:

```
Router# show ip mobile host nai jane@cisco.com

jane@cisco.com
   Allowed lifetime 10:00:00 (36000/default)
   Roam status -Registered-, Home link on interface Loopback0
   Bindings 10.34.253.205
   Accepted 3705, Last time 02/13/03 01:02:37
   Overall service time 6d05h
   Denied 4918, Last time 01/30/03 20:59:14
   Last code 'administratively prohibited (129)'
   Total violations 262
   Tunnel to MN - pkts 0, bytes 0
   Reverse tunnel from MN - pkts 0, bytes 0
```

Table 13 describes the significant fields shown in the display.

Table 13 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 14 describes the significant fields shown in the display.

Table 14 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 secure

To display the mobility security associations for the mobile host, mobile visitor, foreign agent, home agent, or proxy Mobile IP host, use the **show ip mobile secure** command in privileged EXEC mode.

show ip mobile secure {**host** | **visitor** | **foreign-agent** | **home-agent** | **proxy-host** | **summary**} {*ip-address* | **nai** *string*}

Syntax Description

host	Displays security association of the mobile host on the home agent.
visitor	Displays security association of the mobile visitor on the foreign agent.
foreign-agent	Displays security association of the remote foreign agents on the home agent.
home-agent	Displays security association of the remote home agent on the foreign agent.
proxy-host	Displays security association of the proxy mobile user. This keyword is only available on Packet Data Serving Node (PDSN) platforms running specific PDSN code images.
summary	Displays number of security associations in table.
ip-address	IP address.
nai *string*	Network access identifier (NAI).

Command Modes

EXEC

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2(2)XC	The **nai** keyword was added.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.3(4)T	The **proxy-host** keyword was added for PDSN platforms.

Usage Guidelines

Multiple security associations can exist for each entity.

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

Examples

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

```
Router# show ip mobile secure

Security Associations (algorithm,mode,replay protection,key):
10.0.0.6
    SPI 300,  MD5, Prefix-suffix, Timestamp +/- 7,
    Key 00112233445566778899001122334455
```

Table 15 describes the significant fields shown in the display.

Table 15 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 16 describes the significant fields shown in the display.

Table 16 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 16 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 16 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*]

Syntax Description

interface	(Optional) Displays a particular tunnel interface. The *interface* argument is tunnel *x*.

Command Modes

EXEC

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2(13)T	The output was enhanced to display route maps configured on the home agent.
12.2(15)T	The output was enhanced to display tunnel templates for multicast configured on the home agent or mobile router.
12.3(8)T	The output was enhanced to display UDP tunneling.
12.4(9)T	The command was enhanced to display information about multipath support.

Usage Guidelines

This command displays active tunnels created by Mobile IP. When no more users are on the tunnel, the tunnel is released.

Examples

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

```
Router# show ip mobile tunnel

Mobile Tunnels:

Tunnel0:
 src 10.0.0.32, dest 10.0.0.48
 encap IP/IP, mode reverse-allowed, tunnel-users 1
 IP MTU 1480 bytes
 HA created, fast switching enabled, ICMP unreachable enabled
 0 packets input, 0 bytes, 0 drops
 1591241 packets output, 1209738478 bytes
 Route Map is: MoIPMap
Running template configuration for this tunnel:
ip pim sparse-dense-mode
```

The following is sample output from the **show ip mobile tunnel** command that verifies that UDP tunneling is established:

```
Router# show ip mobile tunnel

Mobile Tunnels:
Total mobile ip tunnels 1
Tunnel0:
    src 10.30.30.1, dest 10.10.10.100
    src port 434, dest port 434
    encap MIPUDP/IP, mode reverse-allowed, tunnel-users 1
    IP MTU 1480 bytes
    Path MTU Discovery, mtu: 0, ager: 10 mins, expires: never
    outbound interface Ethernet2/3
    FA created, fast switching disabled, ICMP unreachable enabled
    5 packets input, 600 bytes, 0 drops
    7 packets output, 780 bytes
```

The following is sample output from the **show ip mobile tunnel** command that shows that the mobile node-home agent tunnel is still IP-in-IP, but that the foreign agent-home agent tunnel is UDP:

```
Router# show ip mobile tunnel

Mobile Tunnels:
Total mobile ip tunnels 2
Tunnel0:
 src 10.2.1.1, dest 10.99.100.2
 encap IP/IP, mode reverse-allowed, tunnel-users 1
 IP MTU 1460 bytes
 Path MTU Discovery, mtu: 0, ager: 10 mins, expires: never
 outbound interface Tunnel1
 HA created, fast switching enabled, ICMP unreachable enabled
 11 packets input, 1002 bytes, 0 drops
 5 packets output, 600 bytes

Tunnel1:
 src 10.2.1.1, dest 100.3.1.5
 src port 434, dest port 434
 encap MIPUDP/IP, mode reverse-allowed, tunnel-users 1
 IP MTU 1480 bytes
 Path MTU Discovery, mtu: 0, ager: 10 mins, expires: never
 outbound interface GigabitEthernet0/2
 HA created, fast switching disabled, ICMP unreachable enabled
 11 packets input, 1222 bytes, 0 drops
 7 packets output, 916 bytes
```

The following is sample output from the **show ip mobile tunnel** command that shows that the mobile node has UDP tunneling established with the home agent:

```
Router# show ip mobile tunnel

Total mobile ip tunnels 1
Tunnel0:
 src 10.10.10.100, dest 10.10.10.50
 src port 434, dest port 434
 encap MIPUDP/IP, mode reverse-allowed, tunnel-users 1
 IP MTU 1480 bytes
 Path MTU Discovery, mtu: 0, ager: 10 mins, expires: never
 outbound interface Ethernet2/1
 HA created, fast switching disabled, ICMP unreachable enabled
 5 packets input, 600 bytes, 0 drops
 5 packets output, 600 bytes
```

The following is sample output when the mobile router is configured for multipath support:

```
Router# show ip mobile tunnel

Mobile Tunnels:

Total mobile ip tunnels 1
Tunnel0:
    src 10.1.1.11, dest 10.1.1.10 Key 6
```

```
encap IP/IP, mode reverse-allowed, tunnel-users 1
IP MTU 1480 bytes
Path MTU Discovery, mtu: 0, ager: 10 mins, expires: never
outbound interface Ethernet1/0
MR created, fast switching enabled, ICMP unreachable enabled
4 packets input, 306 bytes, 0 drops
6 packets output, 436 bytes
Template configuration:
    ip pim sparse-dense-mode
```

Table 17 describes the significant fields shown in the display.

Table 17 show ip mobile tunnel Field Descriptions

Field	Description
src	Tunnel source IP address.
dest	Tunnel destination IP address.
Key	Identifies the tunnel when there are multiple tunnels between the same end points (source address and destination address) for multipath support. This situation can occur if a mobile router registers through foreign agents on different interfaces. All of the HA-MR tunnels would have the same end points.
encap	Tunnel encapsulation type.
mode	Either reverse-allowed or reverse-off for reverse tunnel mode.
tunnel-users	Number of users on the tunnel.
HA created	Entity that created the tunnel. This field can be one of three values: HA created, FA created, or MR created.
fast switching	Enabled or disabled.
ICMP unreachable	Enabled or disabled.
packets input	Number of packets in.
bytes	Number of bytes in.
drops	Number of packets dropped. Packets are dropped when there are no visitors to send to after the foreign agent deencapsulates incoming packets. This prevents loops because the foreign agent will otherwise route the de-encapsulated packets back to the home agent.
packets output	Number of packets output.
bytes	Number of bytes output.
Route Map is	Name of the route map.
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 18 describes significant fields shown in the display.

Table 18 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 18 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: • (1) No mobility security association • (2) Bad authenticator • (3) Bad identifier • (4) Bad SPI • (5) Missing security extension • (6) Other

show ip route vrf

To display the IP routing table associated with a Virtual Private Network (VPN) routing and forwarding (VRF) instance, use the **show ip route vrf** command in user EXEC or privileged EXEC mode.

show ip route vrf *vrf-name* [**connected**] [*protocol* [*as-number*] [*tag*] [*output-modifiers*]] [*ip-prefix*] [**list** *number* [*output-modifiers*]] [**profile**] [**static** [*output-modifiers*]] [**summary** [*output-modifiers*]] [**supernets-only** [*output-modifiers*]]

Syntax Description

vrf-name	Name assigned to the VRF.
connected	(Optional) Displays all connected routes in a VRF.
protocol	(Optional) To specify a routing protocol, use one of the following keywords: **bgp**, **egp**, **eigrp**, **hello**, **igrp**, **isis**, **ospf**, or **rip**.
as-number	(Optional) Autonomous system number.
tag	(Optional) Cisco IOS routing area label.
output-modifiers	(Optional) For a list of associated keywords and arguments, use context-sensitive help.
ip-prefix	(Optional) Specifies a network to display.
list *number*	(Optional) Specifies the IP access list to display.
profile	(Optional) Displays the IP routing table profile.
static	(Optional) Displays static routes.
summary	(Optional) Displays a summary of routes.
supernets-only	(Optional) Displays supernet entries only.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(2)T	The *ip-prefix* argument was added. The output from the **show ip route vrf** *vrf-name ip-prefix* command was enhanced to display information on the multipaths to the specified network.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.0(22)S	Enhanced Interior Gateway Routing Protocol (EIGRP) VRF support was added.
12.2(15)T	EIGRP VRF support was integrated into Cisco IOS Release 12.2(15)T.
12.2(18)S	EIGRP VRF support was integrated into Cisco IOS Release 12.2(18)S.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	The output was enhanced to display remote label information and corresponding MPLS flags for prefixes that have remote labels stored in the Routing Information Base (RIB).

Usage Guidelines

This command displays specified information from the IP routing table of a VRF.

Examples

This example shows the IP routing table associated with the VRF named vrf1:

```
Router# show ip route vrf vrf1

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
       U - per-user static route, o - ODR
       T - traffic engineered route

Gateway of last resort is not set

B    10.0.0.0/8 [200/0] via 10.13.13.13, 00:24:19
C    10.0.0.0/8 is directly connected, Ethernet1/3
B    10.0.0.0/8 [20/0] via 10.0.0.1, 02:10:22
B    10.0.0.0/8 [200/0] via 10.13.13.13, 00:24:20
```

This example shows BGP entries in the IP routing table associated with the VRF named vrf1:

```
Router# show ip route vrf vrf1 bgp

B  10.0.0.0/8 [200/0] via 10.13.13.13, 03:44:14
B  10.0.0.0/8 [20/0] via 10.0.0.1, 03:44:12
B  10.0.0.0/8 [200/0] via 10.13.13.13, 03:43:14
```

This example shows the IP routing table associated with a VRF named PATH and network 10.22.22.0:

```
Router# show ip route vrf PATH 10.22.22.0

Routing entry for 10.22.22.0/24
  Known via "bgp 1", distance 200, metric 0
  Tag 22, type internal
  Last update from 10.22.5.10 00:01:07 ago
  Routing Descriptor Blocks:
  * 10.22.7.8 (Default-IP-Routing-Table), from 10.11.3.4, 00:01:07 ago
      Route metric is 0, traffic share count is 1
      AS Hops 1
    10.22.1.9 (Default-IP-Routing-Table), from 10.11.1.2, 00:01:07 ago
      Route metric is 0, traffic share count is 1
      AS Hops 1
    10.22.6.10 (Default-IP-Routing-Table), from 10.11.6.7, 00:01:07 ago
      Route metric is 0, traffic share count is 1
      AS Hops 1
    10.22.4.10 (Default-IP-Routing-Table), from 10.11.4.5, 00:01:07 ago
      Route metric is 0, traffic share count is 1
      AS Hops 1
    10.22.5.10 (Default-IP-Routing-Table), from 10.11.5.6, 00:01:07 ago
      Route metric is 0, traffic share count is 1
      AS Hops 1
```

Table 19 describes the significant fields shown when the **show ip route vrf** *vrf-name ip-prefix* command is used.

Table 19 show ip route vrf Field Descriptions

Field	Description
Routing entry for 10.22.22.0/24	Network number.
Known via ...	Indicates how the route was derived.
distance	Administrative distance of the information source.
metric	The metric to reach the destination network.
Tag	Integer that is used to implement the route.
type	Indicates that the route is an L1 type or L2 type route.
Last update from 10.22.5.10	Indicates the IP address of a router that is the next hop to the remote network and the router interface on which the last update arrived.
00:01:07 ago	Specifies the last time the route was updated (in hours:minutes:seconds).
Routing Descriptor Blocks:	Displays the next hop IP address followed by the information source.
10.22.6.10, from 10.11.6.7, 00:01:07 ago	Indicates the next hop address, the address of the gateway that sent the update, and the time that has elapsed since this update was received (in hours:minutes:seconds).
Route metric	This value is the best metric for this routing descriptor block.
traffic share count	Number of uses for this routing descriptor block.
AS Hops	Number of hops to the destination or to the router where the route first enters internal BGP (iBGP).

Example of Output Using the Cisco IOS Software Modularity for Layer 3 VPNs Feature

The following is sample output from the **show ip route vrf** command on routers using the Cisco IOS Software Modularity for Layer 3 VPNs feature. The output includes remote label information and corresponding MPLS flags for prefixes that have remote labels stored in the RIB, if BGP is the label distribution protocol:

```
Router# show ip route vrf v2 10.2.2.2

Routing entry for 10.2.2.2/32
  Known via "bgp 1", distance 200, metric 0, type internal
  Redistributing via ospf 2
  Advertised by ospf 2 subnets
  Last update from 10.0.0.4 00:22:59 ago
  Routing Descriptor Blocks:
  * 10.0.0.4 (Default-IP-Routing-Table), from 10.0.0.31, 00:22:59 ago
      Route metric is 0, traffic share count is 1
      AS Hops 0
      MPLS label: 1300
      MPLS Flags: MPLS Required
```

Table 20 describes the significant fields shown in the display.

Table 20 show ip route vrf Field Descriptions

Field	Description
MPLS label	Displays the BGP prefix from the BGP peer. The output shows one of the following values: • A label value (16 - 1048575) • A reserved label value, such as explicit-null or implicit-null • The word "none" if no label is received from the peer The MPLS label field does not display if any of the following conditions is true: • BGP is not the LDP. However, OSPF prefixes learned via sham link display an MPLS label. • MPLS is not supported. • The prefix was imported from another VRF, where the prefix was an IGP prefix and LDP provided the remote label for it.
MPLS Flags	The name of one of the following MPLS flags is displayed if any is set: • MPLS Required—Packets are forwarded to this prefix because the MPLS label stack is present. If MPLS is disabled in the outgoing interface, the packets are dropped. • No Global—MPLS packets for this prefix are forwarded from the VRF interface, not from the interface in global table. Using the VRF interface prevents loops in scenarios that use ieBGP multipath. • NSF—The prefix is from an NSF-aware neighbor. If the routing information temporarily disappears due to a disruption in the control plane, packets for this prefix are preserved.

Related Commands

Command	Description
show ip cache	Displays the Cisco Express Forwarding table associated with a VRF.
show ip vrf	Displays the set of defined VRFs and associated interfaces.

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.

standby track decrement priority

To lower the priority of an particular HA in a redundancy scenario, use the **standby track** *tracking object id* **decrement** *priority* command in global configuration mode. To disable this function, use the **no** form of the command.

standby track *tracking object id* **decrement** *priority*

no standby track *tracking object id* **decrement** *priority*

Syntax Description

tracking object id	The name of the specific tracking object.
priority	Specifies the priority level.

Defaults

There are no default values.

Command Modes

Global Configuration

Command History

Release	Modification
12.3(14)YX	This command was introduced.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.

track id application home-agent

To create a tracking object to track the home-agent state, use the **track** *tracking object id* **application home-agent** command in global configuration. To disable this feature, use the **no** form of the command.

track *tracking object id* **application home-agent**

no track *tracking object id* **application home-agent**

Syntax Description

tracking object id	The name of the specific tracking object.

Defaults

There are no default values.

Command Modes

Global Configuration

Command History

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

Examples

The following example illustrates the **track application home-agent** command:

```
router# track tracking object id application home-agent
```

virtual

To configure virtual server attributes, use the **virtual** command in SLB virtual server configuration mode. To remove the attributes, use the **no** form of this command.

Encapsulation Security Payload (ESP) and Generic Routing Encapsulation (GRE) Protocols

virtual *ip-address* [*netmask* [**group**]] {**esp** | **gre** | *protocol*}

no virtual *ip-address* [*netmask* [**group**]] {**esp** | **gre** | *protocol*}

TCP and User Datagram Protocol (UDP)

virtual *ip-address* [*netmask* [**group**]] {**tcp** | **udp**} [*port* | **any**] [**service** *service*]

no virtual *ip-address* [*netmask* [**group**]] {**tcp** | **udp**} [*port* | **any**] [**service** *service*]

Syntax Description

ip-address	IP address for this virtual server instance, used by clients to connect to the server farm.
netmask	(Optional) IP network mask for transparent web cache load balancing. The default is 0.0.0.0 (all subnets).
group	(Optional) Allows the virtual subnet to be advertised. If you do not specify the **group** keyword, the virtual subnet cannot be advertised.
esp	Performs load balancing for only Encapsulation Security Payload (ESP) connections.
gre	Performs load balancing for only Generic Routing Encapsulation (GRE) connections.
protocol	Protocol for which load balancing is performed. The valid range is 2 to 127.
tcp	Performs load balancing for only TCP connections.
udp	Performs load balancing for only User Datagram Protocol (UDP) connections.

port	(Optional) IOS Server Load Balancing (IOS SLB) virtual port (the TCP or UDP port number or port name). If specified, only the connections for the specified port on the server are load-balanced. The ports and the valid name or number for the *port* argument are as follows: • All ports: **any 0** • Connectionless secure Wireless Session Protocol (WSP): **wsp-wtls 9202** • Connectionless WSP: **wsp 9200** • Connection-oriented secure WSP: **wsp-wtp-wtls 9203** • Connection-oriented WSP: **wsp-wtp 9201** • Domain Name System: **dns 53** • File Transfer Protocol: **ftp 21** • General packet radio service (GPRS) tunneling protocol (GTP): **gtp 3386** • HTTP over Secure Socket Layer: **https 443** • Internet Key Exchange (IKE): **isakmp 500** • Mapping of airline traffic over IP, Type A: **matip-a 350** • Network News Transport Protocol: **nntp 119** • Post Office Protocol v2: **pop2 109** • Post Office Protocol v3: **pop3 110** • Simple Mail Transport Protocol: **smtp 25** • Telnet: **telnet 23** • X.25 over TCP (XOT): **xot 1998** • World Wide Web (HTTP): **www 80** Specify a port number of 0 to configure an all-port virtual server (that is, a virtual server that accepts flows destined for all ports except GTP ports).
any	(Optional) Performs load balancing on all ports.
service *service*	(Optional) Couples connections associated with a given service, such as HTTP or Telnet, so all related connections from the same client use the same real server. The following are the valid types of connection coupling: • **ftp**—Couples FTP data connections with the control session that created them. • **gtp**—Enables GPRS load balancing without general packet radio service (GPRS) tunneling protocol (GTP) cause code inspection enabled, which allows load-balancing decisions to be made using Layer 5 information. You can balance UDP flows without awareness of GTP by omitting the **service gtp** keywords. • **gtp-inspect**—Enables GPRS load balancing with GTP cause code inspection enabled. • **ipmobile**—Enables the Home Agent Director. • **per-packet**—Does not maintain connection objects for packets destined for this virtual server. • **radius**—Enables IOS SLB to build RADIUS session objects for RADIUS load balancing.

Defaults

No default behavior or values.

Command Modes

SLB virtual server configuration (config-slb-vserver)

Command History

Release	Modification
12.0(7)XE	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2	This command was integrated into Cisco IOS Release 12.2.
12.1(5a)E	The **wsp**, **wsp-wtp**, **wsp-wtls**, and **wsp-wtp-wtls** keywords were added.
12.1(9)E	The **gtp** option was added as a new value on the *service* argument.
12.1(11b)E	The following keywords, arguments, and options were added: • The **esp**, **gre**, and **all** keywords • The *protocol* argument • The **isakmp** option on the *port* argument • The **per-packet** and **radius** options on the *service* argument The **wsp**, **wsp-wtp**, **wsp-wtls**, and **wsp-wtp-wtls** keywords were changed to options for the *port* argument.
12.1(12c)E	The **group** keyword was added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.1(13)E3	The **gtp-inspect** option was added as a new value on the *service* argument.
12.2(14)ZA2	The **ipmobile** option was added as a new value on the *service* argument.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The **no virtual** command is allowed only if the virtual server was removed from service by the **no inservice** command.

For some applications, it is not feasible to configure all the virtual server TCP or UDP port numbers for IOS SLB. To support such applications, you can configure IOS SLB virtual servers to accept flows destined for all ports. To configure an all-port virtual server, specify a port number of 0 or any.

Note In general, you should use port-bound virtual servers instead of all-port virtual servers. When you use all-port virtual servers, flows can be passed to servers for which no application port exists. When servers reject these flows, IOS SLB might fail the server and remove it from load balancing.

Specifying port 9201 for connection-oriented WSP mode also activates the Wireless Application Protocol (WAP) finite state machine (FSM), which monitors WSP and drives the session FSM accordingly.

In RADIUS load balancing, IOS SLB maintains session objects in a database to ensure that re-sent RADIUS requests are load-balanced to the same real server.

Examples

The following example specifies that the virtual server with the IP address 10.0.0.1 performs load balancing for TCP connections for the port named www. The virtual server processes HTTP requests.

```
Router(config)# ip slb vserver PUBLIC_HTTP
Router(config-slb-vserver)# virtual 10.0.0.1 tcp www
```

The following example specifies that the virtual server with the IP address 10.0.0.13 performs load balancing for UDP connections for all ports. The virtual server processes HTTP requests.

```
Router(config)# ip slb vserver PUBLIC_HTTP
Router(config-slb-vserver)# virtual 10.0.0.13 udp 0
```

Related Commands

Command	Description
ip slb vserver	Identifies a virtual server.
show ip slb vservers	Displays information about the virtual servers defined to IOS Server Load Balancing (IOS SLB).