Cisco Mobile Wireless Home Agent Command Reference for IOS Release 12.4(15)XM2

This section documents new or modified commands. All other commands used with this feature are documented in the Cisco IOS Release 12.4 command reference publications.

aaa accounting

To enable authentication, authorization, and accounting (AAA) accounting of requested services for billing or security purposes when you use RADIUS or TACACS+, use the **aaa accounting** command in global configuration mode. To disable AAA accounting, use the **no** form of this command.

aaa accounting {**auth-proxy** | **system** | **network** | **exec** | **connection** | **commands** *level*} {**default** | *list-name*} {**start-stop** | **stop-only** | **none**} [**broadcast**] **group** *groupname*

no aaa accounting {**auth-proxy** | **system** | **network** | **exec** | **connection** | **commands** *level*} {**default** | *list-name*} [**broadcast**] **group** *groupname*

Syntax Description

auth-proxy	Provides information about all authenticated-proxy user events.
system	Performs accounting for all system-level events not associated with users, such as reloads.
network	Runs accounting for all network-related service requests, including SLIP[1], PPP[2], PPP NCPs[3], and ARAP[4].
exec	Runs accounting for EXEC shell session. This keyword might return user profile information such as what is generated by the **autocommand** command.
connection	Provides information about all outbound connections made from the network access server, such as Telnet, LAT[5], TN3270, PAD[6], and rlogin.
commands *level*	Runs accounting for all commands at the specified privilege level. Valid privilege level entries are integers from 0 through 15.
default	Uses the listed accounting methods that follow this argument as the default list of methods for accounting services.
list-name	Character string used to name the list of at least one of the accounting methods described in Table 3.
start-stop	Sends a “start” accounting notice at the beginning of a process and a “stop” accounting notice at the end of a process. The “start” accounting record is sent in the background. The requested user process begins regardless of whether the “start” accounting notice was received by the accounting server.
stop-only	Sends a “stop” accounting notice at the end of the requested user process.
none	Disables accounting services on this line or interface.
broadcast	(Optional) Enables sending accounting records to multiple AAA servers. Simultaneously sends accounting records to the first server in each group. If the first server is unavailable, fail over occurs using the backup servers defined within that group.
group *groupname*	At least one of the keywords described in Table 2.

1. SLIP = Serial Line Internet Protocol
2. PPP = Point-to-Point Protocol
3. PPP NCPs = Point-to-Point Protocol Network Control Protocols
4. ARAP = AppleTalk Remote Access Protocol
5. LAT = local-area transport
6. PAD = packet assembler/disassembler

Defaults

AAA accounting is disabled.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.
12.0(5)T	Group server support was added.
12.1(1)T	The **broadcast** keyword was added on the Cisco AS5300 and Cisco AS5800 universal access servers.
12.1(5)T	The **auth-proxy** keyword was added.

Usage Guidelines

Use the **aaa accounting** command to enable accounting and to create named method lists defining specific accounting methods on a per-line or per-interface basis.

Table 2 contains descriptions of accounting method keywords.

Table 2 aaa accounting Methods

Keyword	Description
group radius	Uses the list of all RADIUS servers for authentication as defined by the **aaa group server radius** command.
group tacacs+	Uses the list of all TACACS+ servers for authentication as defined by the **aaa group server tacacs+** command.
group *group-name*	Uses a subset of RADIUS or TACACS+ servers for accounting as defined by the server group *group-name*.

In Table 1, the **group radius** and **group tacacs+** methods refer to a set of previously defined RADIUS or TACACS+ servers. Use the **radius-server host** and **tacacs-server host** commands to configure the host servers. Use the **aaa group server radius** and **aaa group server tacacs+** commands to create a named group of servers.

Cisco IOS software supports the following two methods of accounting:

- RADIUS—The network access server reports user activity to the RADIUS security server in the form of accounting records. Each accounting record contains accounting attribute-value (AV) pairs and is stored on the security server.
- TACACS+—The network access server reports user activity to the TACACS+ security server in the form of accounting records. Each accounting record contains accounting attribute-value (AV) pairs and is stored on the security server.

Method lists for accounting define the way accounting will be performed. Named accounting method lists enable you to designate a particular security protocol to be used on specific lines or interfaces for particular types of accounting services. Create a list by entering the *list-name* and the *method*, where *list-name* is any character string used to name this list (excluding the names of methods, such as radius or tacacs+) and *method* identifies the methods to be tried in sequence as given.

If the **aaa accounting** command for a particular accounting type is issued without a named method list specified, the default method list is automatically applied to all interfaces or lines (where this accounting type applies) except those that have a named method list explicitly defined. (A defined method list overrides the default method list.) If no default method list is defined, then no accounting takes place.

Named accounting method lists are specific to the indicated type of accounting. Method list keywords are described in Table 3.

Table 3 aaa accounting Methods Lists

Keyword	Description
auth-proxy	Creates a method list to provide accounting information about all authenticated hosts that use the authentication proxy service.
commands	Creates a method list to provide accounting information about specific, individual EXEC commands associated with a specific privilege level.
connection	Creates a method list to provide accounting information about all outbound connections made from the network access server.
exec	Creates a method list to provide accounting records about user EXEC terminal sessions on the network access server, including username, date, and start and stop times.
network	Creates a method list to provide accounting information for SLIP, PPP, NCPs, and ARA sessions.
resource	Creates a method list to provide accounting records for calls that have passed user authentication or calls that failed to be authenticated.

Note System accounting does not use named accounting lists; you can only define the default list for system accounting.

For minimal accounting, include the **stop-only** keyword to send a "stop" record accounting notice at the end of the requested user process. For more accounting, you can include the **start-stop** keyword, so that RADIUS or TACACS+ sends a "start" accounting notice at the beginning of the requested process and a "stop" accounting notice at the end of the process. Accounting is stored only on the RADIUS or TACACS+ server. The **none** keyword disables accounting services for the specified line or interface.

When AAA accounting is activated, the network access server monitors either RADIUS accounting attributes or TACACS+ AV pairs pertinent to the connection, depending on the security method you have implemented. The network access server reports these attributes as accounting records, which are then stored in an accounting log on the security server. For a list of supported RADIUS accounting attributes, refer to the appendix "RADIUS Attributes" in the *Cisco IOS Security Configuration Guide*. For a list of supported TACACS+ accounting AV pairs, refer to the appendix "TACACS+ Attribute-Value Pairs" in the *Cisco IOS Security Configuration Guide*.

Note This command cannot be used with TACACS or extended TACACS.

Examples

The following example defines a default commands accounting method list, where accounting services are provided by a TACACS+ security server, set for privilege level 15 commands with a stop-only restriction.

```
aaa accounting commands 15 default stop-only group tacacs+
```

The following example defines a default auth-proxy accounting method list, where accounting services are provided by a TACACS+ security server with a stop-only restriction. The **aaa accounting** command activates authentication proxy accounting.

```
aaa new-model
aaa authentication login default group tacacs+
aaa authorization auth-proxy default group tacacs+
aaa accounting auth-proxy default start-stop group tacacs+
```

Related Commands

Command	Description
aaa authentication ppp	Specifies one or more AAA authentication methods for use on serial interfaces running PPP.
aaa authorization	Sets parameters that restrict user access to a network.
aaa group server radius	Groups different RADIUS server hosts into distinct lists and distinct methods.
aaa group server tacacs	Groups different server hosts into distinct lists and distinct methods.
aaa new-model	Enables the AAA access control model.
radius-server host	Specifies a RADIUS server host.
tacacs-server host	Specifies a TACACS+ server host.

aaa accounting update

To enable periodic interim accounting records to be sent to the accounting server, use the **aaa accounting update** command in global configuration mode. To disable interim accounting updates, use the no form of this command.

aaa accounting update [newinfo] [periodic *number***]**

no aaa accounting update

Syntax Description

newinfo	(Optional) Causes an interim accounting record to be sent to the accounting server whenever there is new accounting information to report relating to the user in question.
periodic	(Optional) Causes an interim accounting record to be sent to the accounting server periodically, as defined by the argument number.
number	Integer specifying number of minutes.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
11.3	This command was introduced.

Usage Guidelines

When **aaa accounting update** is activated, the Cisco IOS software issues interim accounting records for all users on the system. If the keyword **newinfo** is used, interim accounting records will be sent to the accounting server every time there is new accounting information to report. An example of this would be when IP Control Protocol (IPCP) completes IP address negotiation with the remote peer. The interim accounting record will include the negotiated IP address used by the remote peer.

When used with the keyword **periodic**, interim accounting records are sent periodically as defined by the argument number. The interim accounting record contains all of the accounting information recorded for that user up to the time the accounting record is sent.

When using both the **newinfo** and **periodic** keywords, interim accounting records are sent to the accounting server every time there is new accounting information to report, and accounting records are sent to the accounting server periodically as defined by the argument number. For example, if you configure a**aa accounting update newinfo periodic** *number*, all users currently logged in will continue to generate periodic interim accounting records while new users will generate accounting records based on the newinfo algorithm.

Caution Using the **aaa accounting update periodic** command can cause heavy congestion when many users are logged in to the network.

Examples

The following example sends PPP accounting records to a remote RADIUS server. When IPCP completes negotiation, this command sends an interim accounting record to the RADIUS server that includes the negotiated IP address for this user; it also sends periodic interim accounting records to the RADIUS server at 30 minute intervals.

```
aaa accounting network default start-stop group radius
aaa accounting update newinfo periodic 30
```

Related Commands

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

aaa authorization ipmobile

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

aaa authorization ipmobile {**tacacs+** | **radius**}

no aaa authorization ipmobile {**tacacs+** | **radius**}

Syntax Description

tacacs+	Use TACACS+.
radius	Use RADIUS.

Defaults

AAA is not used to retrieve security associations for authentication.

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

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

Examples

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

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

Related Commands

Command	Description
show ip mobile host	Displays the mobility host information.

aaa pod server

To enable inbound user sessions to be disconnected when specific session attributes are presented, use the **aaa pod server** global configuration command. To disable this feature, use the **no** form of this command.

aaa pod server [port *port-number***] [auth-type {any | all | session-key}] server-key** *string*

no aaa pod server

Syntax Description

port port-number	(Optional) The network access server port to use for packet of disconnect requests. If no port is specified, port 1700 is used.
auth-type	(Optional) The type of authorization required for disconnecting sessions. If no authentication type is specified, auth-type is the default.
any	(Optional) Specifies that the session that matches all attributes sent in the POD packet is disconnected. The POD packet can contain one or more of four key attributes (user-name, framed-IP-address, session-ID, and session-key).
all	(Optional) Only a session that matches all four key attributes is disconnected. All is the default.
session-key	(Optional) Specifies that the session that has a matching session-key attribute is disconnected. All other attributes are ignored.
server-key *string*	The secret text string that is shared between the network access server and the client workstation. This secret string must be the same on both systems.

Defaults

The POD server function is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.

Usage Guidelines

For a session to be disconnected, the values in one or more of the key fields in the POD request must match the values for a session on one of the network access server ports. Which values must match depends on the auth-type attribute defined in the command. If no auth-type is specified, all four values must match. If no match is found, all connections remain intact and an error response is returned. The key fields are as follows:

- User-Name
- Framed-IP-Address
- Session-Id
- Server-Key

Examples

The following example enables POD and sets the secret key to “ab9123.”

```
router (config)# aaa pod server server-key ab9123
```

access list

To configure the access list mechanism for filtering frames by protocol type or vendor code, use the **access-list** global configuration command. Use the **no** form of this command to remove the single specified entry from the access list.

access-list *access-list-number* **{permit | deny}** {*type-code wild-mask* | *address mask*}

no access-list *access-list-number* **{permit | deny}** {*type-code wild-mask* | *address mask*}

Syntax Description

access-list-number	Integer that identifies the access list. If the type-code wild-mask arguments are included, this integer ranges from 200 to 299, indicating that filtering is by protocol type. If the address and mask arguments are included, this integer ranges from 700 to 799, indicating that filtering is by vendor code.
permit	Permits the frame.
deny	Denies the frame.
type-code	16-bit hexadecimal number written with a leading 0x; for example, 0x6000. Specify either a Link Service Access Point (LSAP) type code for 802-encapsulated packets or a SNAP type code for SNAP-encapsulated packets. (LSAP, sometimes called SAP, refers to the type codes found in the DSAP and SSAP fields of the 802 header.)
wild-mask	16-bit hexadecimal number whose ones bits correspond to bits in the type-code argument. The wild-mask indicates which bits in the type-code argument should be ignored when making a comparison. (A mask for a DSAP/SSAP pair should always be 0x0101 because these two bits are used for purposes other than identifying the SAP code.)
address	48-bit Token Ring address written in dotted triplet form. This field is used for filtering by vendor code.
mask	48-bit Token Ring address written in dotted triplet form. The ones bits in mask are the bits to be ignored in address. This field is used for filtering by vendor code.

Defaults

No numbered encryption access lists are defined, and therefore no traffic will be encrypted/decrypted. After being defined, all encryption access lists contain an implicit “deny” (“do not encrypt/decrypt”) statement at the end of the list..

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

Use encryption access lists to control which packets on an interface are encrypted/decrypted, and which are transmitted as plain text (unencrypted).

When a packet is examined for an encryption access list match, encryption access list statements are checked in the order that the statements were created. After a packet matches the conditions in a statement, no more statements will be checked. This means that you need to carefully consider the order in which you enter the statements.

To use the encryption access list, you must first specify the access list in a crypto map and then apply the crypto map to an interface, using the crypto map (CET global configuration) and crypto map (CET interface configuration) commands.

Fragmented IP packets, other than the initial fragment, are immediately accepted by any extended IP access list. Extended access lists used to control virtual terminal line access or restrict contents of routing updates must not match the TCP source port, the type of service value, or the packet's precedence.

Note After an access list is created initially, any subsequent additions (possibly entered from the terminal) are placed at the end of the list. You cannot selectively add or remove access list command lines from a specific access list.

Caution When creating encryption access lists, we do not recommend using the any keyword to specify source or destination addresses. Using the any keyword with a permit statement could cause extreme problems if a packet enters your router and is destined for a router that is not configured for encryption. This would cause your router to attempt to set up an encryption session with a nonencrypting router. If you incorrectly use the any keyword with a deny statement, you might inadvertently prevent all packets from being encrypted, which could present a security risk.

Note If you view your router's access lists by using a command such as show ip access-list, all extended IP access lists will be shown in the command output. This includes extended IP access lists that are used for traffic filtering purposes as well as those that are used for encryption. The show command output does not differentiate between the two uses of the extended access lists.

Examples

The following example creates a numbered encryption access list that specifies a class C subnet for the source and a class C subnet for the destination of IP packets. When the router uses this encryption access list, all TCP traffic that is exchanged between the source and destination subnets will be encrypted.

```
access-list 101 permit tcp 172.21.3.0 0.0.0.255 172.22.2.0 0.0.0.255
```

clear ip mobile binding

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

clear ip mobile binding {**all** [**load** *standby-group-name*] | *ip-address* | **nai** *string ip_address* | **vrf realm** *realm*} [**synch**]

Syntax Description

all	Clears all mobility bindings.
load *standby-group-name*	(Optional) Downloads mobility bindings for a standby group after clear.
ip-address	IP address of a mobile node.
nai *string*	Network access identifier of the mobile node.
vrf realm *realm*	The specified vrf realm.
synch	(Optional) Specifies that the bindings that are administratively cleared on the active HA are synched to the standby HA, and the bindings will be deleted on the standby HA

Command Modes

EXEC

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.1(3)T	The following keywords and argument were added: • **all** • **load** • *standby-group-name*
12.2(2)XC	The **nai** keyword and associated variables were added.
12.3(7)XJ	The **vrf realm** keyword and associated variable were added.
12.3(7)XJ1	The **synch** option was added.

Usage Guidelines

The Home Agent creates a mobility binding for each roaming mobile node. The mobility binding allows the mobile node to exchange packets with the correspondent node. Associated with the mobility binding is the tunnel to the visited network and a host route to forward packets destined for the mobile node. There should be no need to clear the binding because it expires after lifetime is reached or when the mobile node deregisters.

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

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

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

Examples

The following example administratively stops mobile node 10.0.0.1 from roaming:

```
Router# clear ip mobile binding 10.0.0.1

Router# show ip mobile binding

Mobility Binding List:
Total 1
10.0.0.1:
    Care-of Addr 68.0.0.31, Src Addr 68.0.0.31,
    Lifetime granted 02:46:40 (10000), remaining 02:46:32
    Flags SbdmGvt, Identification B750FAC4.C28F56A8,
    Tunnel100 src 66.0.0.5 dest 68.0.0.31 reverse-allowed
    Routing Options - (G)GRE
```

Related Commands

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

clear ip mobile host-counters

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

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

Syntax Description

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

Command Modes

EXEC

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2(2)XC	The **nai** keyword and associated variables were added.
12.4(15)XM	Added support to clear HA policing statistics.

Usage Guidelines

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

Examples

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

```
Router# show ip mobile host

20.0.0.1:
    Allowed lifetime 10:00:00 (36000/default)
    Roaming status -Unregistered-, Home link on virtual network 20.0.0.0/8
    Accepted 0, Last time -never-
    Overall service time -never-
    Denied 0, Last time -never-
    Last code '-never- (0)'
    Total violations 0
    Tunnel to MN - pkts 0, bytes 0
    Reverse tunnel from MN - pkts 0, bytes 0


Router# clear ip mobile host-counters
Router# show ip mobile host-counters

20.0.0.1:
    Allowed lifetime 10:00:00 (36000/default)
    Roaming status -Unregistered-, Home link on virtual network 20.0.0.0/8
    Accepted 0, Last time -never-
    Overall service time -never-
    Denied 0, Last time -never-
    Last code '-never- (0)'
    Total violations 0
```

```
Tunnel to MN - pkts 0, bytes 0
Reverse tunnel from MN - pkts 0, bytes 0
```

Related Commands

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

clear ip mobile secure

To clear and retrieve remote security associations, use the **clear ip mobile secure** EXEC command.

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

Syntax Description

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

Command Modes

EXEC

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2(2)XC	The **nai** keyword and associated variables were added.

Usage Guidelines

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

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

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

You can use the **clear ip mobile secure all** command clears all the keys MN, FA and HA-RK, generated and downloaded from AAA.

Examples

In the following example, the AAA server has the security association for user 10.0.0.1 after registration:

```
Router# show ip mobile secure host 10.0.0.1

Security Associations (algorithm,mode,replay protection,key):
10.0.0.1:
    SPI 300,  MD5, Prefix-suffix, Timestamp +/- 7,
    Key 'oldkey' 1230552d39b7c1751f86bae5205ec0c8
```

The security association of the AAA server changes as follows:

```
Router# clear ip mobile secure host 10.0.0.1 load

Router# show ip mobile secure host 10.0.0.1

10.0.0.1:
    SPI 300,  MD5, Prefix-suffix, Timestamp +/- 7,
    Key 'newkey' 1230552d39b7c1751f86bae5205ec0c8
```

Related Commands

Command	Description
ip mobile secure	Specifies the mobility security associations for mobile host, visitor, Home Agent, and Foreign Agent.

clear ip mobile traffic

To clear counters, use the **clear ip mobile traffic** Privileged EXEC command.

clear 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.
12.3(7)XJ	This command adds clear MIPv4 Registration Revocation related counters and Radius Disconnect related statistics.
12.4(15)XM	Added the abilility to clear Hotlining counters, and MIP-LAC counters.

Usage Guidelines

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

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

Examples

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

```
Router# show ip mobile traffic

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

Router# show ip mobile traffic

IP Mobility traffic:
Advertisements:
    Solicitations received 0
    Advertisements sent 0, response to solicitation 0
Home Agent Registrations:
    Register 0, Deregister 0 requests
```

```
Register 0, Deregister 0 replied
Accepted 0, No simultaneous bindings 0
Denied 0, Ignored 0
Unspecified 0, Unknown HA 0
Administrative prohibited 0, No resource 0
Authentication failed MN 0, FA 0
Bad identification 0, Bad request form 0
```

Related Commands

Command	Description
show ip mobile traffic	Displays the protocol counters.

crypto map (global IPSec)

To create or modify a crypto map entry and enter the crypto map configuration mode, use the **crypto map** global configuration command. To delete a crypto map entry or set, use the no form of this command.

crypto map *map-name seq-num* **ipsec-manual**

crypto map *map-name seq-num* **ipsec-isakmp** [**dynamic** *dynamic-map-name*] [**discover**]

no crypto map *map-name* [*seq-num*]

Syntax Description

map name	The name you assign to the crypto map set
seq-num	The number you assign to the crypto map entry.
ipsec-manual	Indicates that IKE will not be used to establish the IPSec security associations for protecting the traffic specified by this crypto map entry.
ipsec-isakmp	Indicates that IKE will be used to establish the IPSec security associations for protecting the traffic specified by this crypto map entry.
dynamic	(Optional) Specifies that this crypto map entry is to reference a preexisting dynamic crypto map. Dynamic crypto maps are policy templates used in processing negotiation requests from a peer IPSec device. If you use this keyword, none of the crypto map configuration commands will be available.
dynamic-map-name	(Optional) Specifies the name of the dynamic crypto map set that should be used as the policy template.
discover	(Optional) Enables peer discovery. By default, peer discovery is not enabled.

Command Modes

Global configuration.

Command History

Release	Modification
12.1(1)T	This command was introduced.

Usage Guidelines

Issue the **crypto map** *map-name seq-num* command without a keyword to modify an existing crypto map entry.

Examples

The following example creates a crypto map entry and indicates that IKE will not be used to establish the IPSec security associations for protecting the traffic:

```
Router# crypto map map-name seq-num ipsec-manual
```

debug aaa accounting

To display information on accountable events as they occur, use the **debug aaa accounting** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug aaa accounting

no debug aaa accounting

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Usage Guidelines

The information displayed by the **debug aaa accounting** command is independent of the accounting protocol used to transfer the accounting information to a server. Use the **debug tacacs** and **debug radius** protocol-specific commands to get more detailed information about protocol-level issues.

You can also use the **show accounting** command to step through all active sessions and to print all the accounting records for actively accounted functions. The **show accounting** command allows you to display the active "accountable events" on the system. It provides systems administrators a quick look at what is happening, and may also be useful for collecting information in the event of a data loss of some kind on the accounting server. The **show accounting** command displays additional data on the internal state of the authentication, authorization, and accounting (AAA) security system if **debug aaa accounting** is turned on as well.

Examples

The following is sample output from the **debug aaa accounting** command:

```
Router# debug aaa accounting
16:49:21: AAA/ACCT: EXEC acct start, line 10
16:49:32: AAA/ACCT: Connect start, line 10, glare
16:49:47: AAA/ACCT: Connection acct stop:
task_id=70 service=exec port=10 protocol=telnet address=172.31.3.78 cmd=glare bytes_in=308
bytes_out=76 paks_in=45 paks_out=54 elapsed_time=14
```

debug aaa authentication

To display information on authentication, authorization, and accounting (AAA) TACACS+ authentication, use the **debug aaa authentication** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug aaa authentication

no debug aaa authentication

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Usage Guidelines

Use this command to learn the methods of authentication being used and the results of these methods.

Examples

The following is sample output from the **debug aaa authentication** command. A single EXEC login that uses the "default" method list and the first method, TACACS+, is displayed. The TACACS+ server sends a GETUSER request to prompt for the username and then a GETPASS request to prompt for the password, and finally a PASS response to indicate a successful login. The number 50996740 is the session ID, which is unique for each authentication. Use this ID number to distinguish between different authentications if several are occurring concurrently.

```
Router# debug aaa authentication

6:50:12: AAA/AUTHEN: create_user user='' ruser='' port='tty19' rem_addr='172.31.60.15'
authen_type=1 service=1 priv=1
6:50:12: AAA/AUTHEN/START (0): port='tty19' list='' action=LOGIN service=LOGIN
6:50:12: AAA/AUTHEN/START (0): using "default" list
6:50:12: AAA/AUTHEN/START (50996740): Method=TACACS+
6:50:12: TAC+ (50996740): received authen response status = GETUSER
6:50:12: AAA/AUTHEN (50996740): status = GETUSER
6:50:15: AAA/AUTHEN/CONT (50996740): continue_login
6:50:15: AAA/AUTHEN (50996740): status = GETUSER
6:50:15: AAA/AUTHEN (50996740): Method=TACACS+
6:50:15: TAC+: send AUTHEN/CONT packet
6:50:15: TAC+ (50996740): received authen response status = GETPASS
6:50:15: AAA/AUTHEN (50996740): status = GETPASS
6:50:20: AAA/AUTHEN/CONT (50996740): continue_login
6:50:20: AAA/AUTHEN (50996740): status = GETPASS
6:50:20: AAA/AUTHEN (50996740): Method=TACACS+
6:50:20: TAC+: send AUTHEN/CONT packet
6:50:20: TAC+ (50996740): received authen response status = PASS
6:50:20: AAA/AUTHEN (50996740): status = PASS
```

debug aaa pod

To display debug information for Radius Disconnect message processing at AAA subsystem level , use the **debug aaa pod** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug aaa pod

no debug aaa pod

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

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

Examples

The following is sample output from the **debug aaa pod** command:

```
Router#sh debugging
General OS:
  AAA POD packet processing debugging is on
```

The scenario is a POD request is received from RADIUS 17.17.17.18 with the set of attributes displayed below and after processing PDSN sends back an ACK

```
Router#
03:30:05: POD: 17.17.17.18 request queued
03:30:05:  ++++++ POD Attribute List ++++++
03:30:05: 63ECE94C 0 00000009 username(336) 12 sri-sip-user
03:30:05: 65FCEB50 0 00000009 clid(27) 11 00000000001
03:30:05: 65FCEB64 0 00000021 cdma-disconnect-reason(420) 4 1(1)
03:30:05: 65FCEB78 0 00000029 cdma-correlation-id(374) 8 00000002
03:30:05:
03:30:05: POD: Sending ACK from port 1700 to 17.17.17.18/1700
```

debug condition

To limit output for some debug commands based on specified conditions, use the **debug condition** command in privileged EXEC mode. To remove the specified condition, use the **no** form of this command.

debug condition {username *username* **| called** *dial-string* **| caller** *dial-string* **| vcid** *vc-id* **| ip** *ip-address* **| calling** *tid/imsi string***]}**

no debug condition {*condition-id* **| all}**

Syntax Description

username *username*	Generates debugging messages for interfaces with the specified username.
called *dial-string*	Generates debugging messages for interfaces with the called party number.
caller *dial-string*	Generates debugging messages for interfaces with the calling party number.
vcid *vc-id*	Generates debugging messages for the VC ID specified.
ip *ip-address*	Generates debugging messages for the IP address specified.
calling *tid/imsi string*	Displays events related to general packet radio service (GPRS) tunneling protocol (GTP) processing on the gateway GPRS support node (GGSN) based on the tunnel identifier (TID) or international mobile system identifier (IMSI) in a Packet Data Protocol (PDP) Context Create Request message.
condition-id	Removes the condition indicated.
all	Removes all debugging conditions, and conditions specified by the debug condition interface command. Use this keyword to disable conditional debugging and reenable debugging for all interfaces.

Defaults

All debugging messages for enabled protocol-specific debug commands are generated.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3(2)AA	This command was introduced.
12.0(23)S	This command was integrated into Cisco IOS Release 12.0(23)S. This command was updated with the vcid and ip keywords to support the debugging of Any Transport over MPLS (AToM) messages.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(15)T	This command was integrated into Cisco IOS Relese 12.2(15)T.
12.3(2)XB	This command was introduced on the GGSN.
12.3(8)T	The **calling** keyword and *tid/imsi string* argument were added.

Usage Guidelines

Use the **debug condition** command to restrict the debug output for some commands. If any **debug condition** commands are enabled, output is only generated for interfaces associated with the specified keyword. In addition, this command enables debugging output for conditional debugging events. Messages are displayed as different interfaces meet specific conditions.

If multiple **debug condition** commands are enabled, output is displayed if at least one condition matches. All the conditions do not need to match.

The **no** form of this command removes the debug condition specified by the condition identifier. The condition identifier is displayed after you use a **debug condition** command or in the output of the **show debug condition** command. If the last condition is removed, debugging output resumes for all interfaces. You will be asked for confirmation before removing the last condition or all conditions.

Not all debugging output is affected by the **debug condition** command. Some commands generate output whenever they are enabled, regardless of whether they meet any conditions. The commands that are affected by the debug condition commands are generally related to dial access functions, where a large amount of output is expected. Output from the following commands is controlled by the debug condition command:

- **debug aaa** {**accounting** | **authorization** | **authentication**}
- **debug dialer events**
- **debug isdn** {**q921** | **q931**}
- **debug modem** {**oob** | **trace**}
- **debug ppp** {**all** | **authentication** | **chap** | **error** | **negotiation** | **multilink events** | **packet**}

Ensure that you enable TID/IMSI-based conditional debugging by entering **debug condition calling** before configuring **debug gprs gtp** and **debug gprs charging**. In addition, ensure that you disable the **debug gprs gtp** and **debug gprs charging** commands using the **no debug all** command before disabling conditional debugging using the **no debug condition** command. This will prevent a flood of debugging messages when you disable conditional debugging.

Examples

Example 1

In the following example, the router displays debugging messages only for interfaces that use a username of fred. The condition identifier displayed after the command is entered identifies this particular condition.

```
Router# debug condition username fred

Condition 1 set
```

Example 2

The following example specifies that the router should display debugging messages only for VC 1000:

```
Router# debug condition vcid 1000

Condition 1 set

01:12:32: 1000 Debug: Condition 1, vcid 1000 triggered, count 1

01:12:32: 1000 Debug: Condition 1, vcid 1000 triggered, count 1
```

Other debugging commands are enabled, but they will only display debugging for VC 1000.

```
Router# debug mpls l2transport vc event
```

```
AToM vc event debugging is on

Router# debug mpls l2transport vc fsm

AToM vc fsm debugging is on
```

The following commands shut down the interface where VC 1000 is established.

```
Router(config)# interface s3/1/0

Router(config-if)# shut
```

The debugging output shows the change to the interface where VC 1000 is established.

```
01:15:59: AToM MGR [13.13.13.13, 1000]: Event local down, state changed from established
to remote ready

01:15:59: AToM MGR [13.13.13.13, 1000]: Local end down, vc is down

01:15:59: AToM SMGR [13.13.13.13, 1000]: Processing imposition update, vc_handle 6227BCF0,
update_action 0, remote_vc_label 18

01:15:59: AToM SMGR [13.13.13.13, 1000]: Imposition Disabled

01:15:59: AToM SMGR [13.13.13.13, 1000]: Processing disposition update, vc_handle
6227BCF0, update_action 0, local_vc_label 755

01:16:01:%LINK-5-CHANGED: Interface Serial3/1/0, changed state to administratively down

01:16:02:%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial3/1/0, changed state to
down
```

debug ip mobile

To display IP mobility activities, use the **debug ip mobil**e command in privileged EXEC mode.

debug ip mobile [advertise | dfp | host [*access-list-number***] | local-area | redundancy | router | upd-tunneling | vpdn-tunneling]**

Syntax Description

advertise	(Optional) Mobility Agent advertisement information.
dfp	(Optional) DFP Agent.
host	(Optional) The mobile host activity.
access-list-number	(Optional) The number of an IP access list.
local-area	(Optional) The local area.
redundancy	(Optional) Mobile redundancy activities.
router	(Optional) Mobile router activities.
upd-tunneling	(Optional) UDP tunneling.
vpdn-tunneling	(Optional) VPDN tunneling.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.0(2)T	The standby keyword was added.
12.2(13)T	This command was enhanced to display information about Foreign Agent reverse tunnels and the mobile networks attached to the mobile router.
12.3(7)XJ	This command is enhanced to include the Resource Management capability.

Usage Guidelines

Use the **debug ip mobile redundancy** command to troubleshoot redundancy problems.

No per-user debugging output is shown for mobile nodes using the network access identifier (NAI) for the **debug ip mobile host** command. Debugging of specific mobile nodes using an IP address is possible through the access list.

Examples

The following is sample output from the debug ip mobile command when Foreign Agent reverse tunneling is enabled:

```
MobileIP:MN 14.0.0.30 deleted from ReverseTunnelTable of Ethernet2/1(Entries 0)
```

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

```
Router# debug ip mobile ?
advertise Mobility Agent advertisements
dfp DFP Agent
host Mobile host activities
local-area Local area mobility
redundancy Mobile redundancy activities
router Mobile router activities
udp-tunneling UDP Tunneling
vpdn-tunneling VPDN Tunneling
```

The following is sample output from the **debug ip mobile advertise** command:

```
debug ip mobile advertise
MobileIP: Agent advertisement sent out Ethernet1/2: type=16, len=10, seq=1,
lifetime=36000,
flags=0x1400(rbhFmGv-rsv-),
Care-of address: 68.0.0.31
Prefix Length ext: len=1 (8 )
FA Challenge value:769C808D
```

Table 4 Debug IP Mobile Advertise Field Descriptions

Field	Description
type	Type of advertisement.
len	Length of extension in bytes.
seq	Sequence number of this advertisement.
lifetime	Lifetime in seconds.
flags	Capital letters represent bits that are set, lower case letters represent unset bits.
Care-of address	IP address.
Prefix Length ext	Number of prefix lengths advertised. This is the bits in the mask of the interface sending this advertisement. Used for roaming detection.

The following is sample output from the **debug ip mobile udp-tunneling** command:

```
Router# debug ip mobile udp-tunneling

  MobileIP: Received UDP Keep-Alive message from tunnel 7.0.0.2:434 - 7.0.0.15:16
  MobileIP: Sending UDP Keep-Alive message for tunnel 7.0.0.2:434 - 7.0.0.15:16
  MobileIP: MN 40.0.0.101 - HA rcv BindUpdAck accept from 7.0.0.67 HAA 7.0.0.2
  MobileIP: UDP Keep-Alive check point time for tunnel 7.0.0.2:434 - 7.0.0.15:16
```

debug ip mobile host

Use the **debug ip mobile host** EXEC command to display IP mobility events.

debug ip mobile host *acl* **[nai]**

no debug ip mobile host [nai]

Syntax Description

acl	(Optional) Access list. The values are 1-99.
nai	(Optional) Mobile host identified by NAI.

Defaults

No default values.

Command History

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

Examples

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

```
Router# debug ip mobile host

MobileIP: HA received registration for MN 20.0.0.6 on interface Ethernet1 using COA
68.0.0.31 HA 66.0.0.5 lifetime 30000 options sbdmgvT
MobileIP: Authenticated FA 68.0.0.31 using SPI 110 (MN 20.0.0.6)
MobileIP: Authenticated MN 20.0.0.6 using SPI 300

MobileIP: HA accepts registration from MN 20.0.0.6
MobileIP: Mobility binding for MN 20.0.0.6 updated
MobileIP: Roam timer started for MN 20.0.0.6, lifetime 30000
MobileIP: MH auth ext added (SPI 300) in reply to MN 20.0.0.6
MobileIP: HF auth ext added (SPI 220) in reply to MN 20.0.0.6

MobileIP: HA sent reply to MN 20.0.0.6
```

debug ip mobile redundancy

Use the **debug ip mobile redundancy** EXEC command to display IP mobility events.

debug ip mobile redundancy

no debug ip mobile redundancy

Syntax Description

This command has no keywords or arguments.

Defaults

No default values.

Command History

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

Examples

The following is sample output from the **debug ip mobile redundancy** command:

```
Router# debug ip mobile redundancy

00:19:21: MobileIP: Adding MN service flags to bindupdate
00:19:21: MobileIP:  Adding MN service flags 0 init registration flags 1
00:19:21: MobileIP: Adding a hared version cvse - bindupdate
00:19:21: MobileIP: HARelayBindUpdate version number 2MobileIP: MN 40.0.0.20 - sent
BindUpd to HA 7.0.0.3 HAA 7.0.0.4
00:19:21: MobileIP: HA standby maint started - cnt 1
00:19:21: MobileIP: MN 40.0.0.20 - HA rcv BindUpdAck accept from 7.0.0.3 HAA 7.0.0.4
00:19:22: MobileIP: HA standby maint started - cnt 1
```

debug ip mobile vpdn-tunnel

To display debugging output for the MIP-LAC feature, use the **debug ip mobile vpdn-tunnel** command in Privileged EXEC mode. Use the **no** form of the command to disable the feature.

debug ip mobile vpdn-tunnel [**events** | **detail**]

no debug ip mobile vpdn-tunnel [**events** | **detail**]

Syntax Description

events	Displays MIP-LAC debugging events.
detail	Displays MIP-LAC debugging details.

Defaults

There are no default values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(15)XM	This command was introduced.

Examples

The following example displays debugging output for the **debug ip mobile vpdn-tunnel detail** command:

```
Router# debug ip mobile vpdn-tunnel detail
```

debug radius

To display information associated with RADIUS, use the **debug radius** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug radius [accounting | authentication | brief | elog | failover | retransmit | verbose]

no debug radius [accounting | authentication | brief | elog | failover | retransmit | verbose]

Syntax Description

accounting	(Optional) RADIUS accounting packets only
authentication	(Optional) RADIUS authentication packets only
brief	(Optional) Displays abbreviated debug output. brief Only I/O transactions are recorded.
elog	(Optional) RADIUS event logging.
failover	(Optional) Packets sent upon fail-over
retransmit	(Optional) Retransmission of packets
verbose	(Optional) Include non essential RADIUS debugs

Defaults

Debugging output in ASCII format is enabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.2(1)T	This command was introduced.
12.2(11)T	The **brief** and **hex** keywords were added. The default output format became ASCII rather than hexadecimal.

Usage Guidelines

RADIUS is a distributed security system that secures networks against unauthorized access. Cisco supports RADIUS under the authentication, authorization, and accounting (AAA) security system. When RADIUS is used on the router, you can use the **debug radius** command to display detailed debugging and troubleshooting information in ASCII format. Use the **debug radius brief** command for abbreviated output displaying client/server interaction and minimum packet information. Use the **debug radius hex** command to display packet dump information that has not been truncated in hex format.

Examples

The following is sample output from the **debug radius** command:

```
Router# debug radius
Radius protocol debugging is on
Radius packet hex dump debugging is off
Router#
00:02:50: RADIUS: ustruct sharecount=3
00:02:50: Radius: radius_port_info() success=0 radius_nas_port=1
```

```
00:02:50: RADIUS: Initial Transmit ISDN 0:D:23 id 0 10.0.0.1:1824, Accounting-Request, len
358
00:02:50: RADIUS: NAS-IP-Address [4] 6 10.0.0.0
00:02:50: RADIUS: Vendor, Cisco [26] 19 VT=02 TL=13 ISDN 0:D:23
00:02:50: RADIUS: NAS-Port-Type [61] 6 Async
00:02:50: RADIUS: User-Name [1] 12 "4085554206"
00:02:50: RADIUS: Called-Station-Id [30] 7 "52981"
00:02:50: RADIUS: Calling-Station-Id [31] 12 "4085554206"
00:02:50: RADIUS: Acct-Status-Type [40] 6 Start
00:02:50: RADIUS: Service-Type [6] 6 Login
00:02:50: RADIUS: Vendor, Cisco [26] 27 VT=33 TL=21 h323-gw-id=5300_43.
00:02:50: RADIUS: Vendor, Cisco [26] 55 VT=01 TL=49 h323-incoming-conf-id=8F3A3163
B4980003 0 29BD0
00:02:50: RADIUS: Vendor, Cisco [26] 31 VT=26 TL=25 h323-call-origin=answer
00:02:50: RADIUS: Vendor, Cisco [26] 32 VT=27 TL=26 h323-call-type=Telephony
00:02:50: RADIUS: Vendor, Cisco [26] 57 VT=25 TL=51 h323-setup-time=*16:02:48.681 PST Fri
Dec 31 1999
00:02:50: RADIUS: Vendor, Cisco [26] 46 VT=24 TL=40 h323-conf-id=8F3A3163 B4980003 0 29BD0
00:02:50: RADIUS: Acct-Session-Id [44] 10 "00000002"
00:02:50: RADIUS: Delay-Time [41] 6 0
00:02:51: RADIUS: Received from id 0 1.7.157.1:1824, Accounting-response, len 20
00:02:51: %ISDN-6-CONNECT: Interface Serial0:22 is now connected to 4085274206
00:03:01: RADIUS: ustruct sharecount=3
00:03:01: Radius: radius_port_info() success=0 radius_nas_port=1
00:03:01: RADIUS: Initial Transmit ISDN 0:D:23 id 1 1.7.157.1:1823, Access-Request, len
171
00:03:01: RADIUS: NAS-IP-Address [4] 6 10.0.0.0
00:03:01: RADIUS: Vendor, Cisco [26] 19 VT=02 TL=13 ISDN 0:D:23
00:03:01: RADIUS: NAS-Port-Type [61] 6 Async
00:03:01: RADIUS: User-Name [1] 8 "123456"
00:03:01: RADIUS: Vendor, Cisco [26] 46 VT=24 TL=40 h323-conf-id=8F3A3163 B4980003 0 29BD0
00:03:01: RADIUS: Calling-Station-Id [31] 12 "4085554206"
00:03:01: RADIUS: User-Password [2] 18 *
00:03:01: RADIUS: Vendor, Cisco [26] 36 VT=01 TL=30 h323-ivr-out=transactionID:0
00:03:01: RADIUS: Received from id 1 1.7.157.1:1823, Access-Accept, len 115
00:03:01: RADIUS: Service-Type [6] 6 Login
00:03:01: RADIUS: Vendor, Cisco [26] 29 VT=101 TL=23 h323-credit-amount=45
00:03:01: RADIUS: Vendor, Cisco [26] 27 VT=102 TL=21 h323-credit-time=33
00:03:01: RADIUS: Vendor, Cisco [26] 26 VT=103 TL=20 h323-return-code=0
00:03:01: RADIUS: Class [25] 7 6C6F63616C
00:03:01: RADIUS: saved authorization data for user 62321E14 at 6233D258
00:03:13: %ISDN-6-DISCONNECT: Interface Serial0:22 disconnected from 4085274206, call
lasted 22 seconds
00:03:13: RADIUS: ustruct sharecount=2
00:03:13: Radius: radius_port_info() success=0 radius_nas_port=1
00:03:13: RADIUS: Sent class "local" at 6233D2C4 from user 62321E14
00:03:13: RADIUS: Initial Transmit ISDN 0:D:23 id 2 1.7.157.1:1824, Accounting-Request,
len 775
00:03:13: RADIUS: NAS-IP-Address [4] 6 10.0.0.0
00:03:13: RADIUS: Vendor, Cisco [26] 19 VT=02 TL=13 ISDN 0:D:23
00:03:13: RADIUS: NAS-Port-Type [61] 6 Async
00:03:13: RADIUS: User-Name [1] 8 "123456"
00:03:13: RADIUS: Called-Station-Id [30] 7 "52981"
00:03:13: RADIUS: Calling-Station-Id [31] 12 "4085274206"
00:03:13: RADIUS: Acct-Status-Type [40] 6 Stop
00:03:13: RADIUS: Class [25] 7 6C6F63616C
00:03:13: RADIUS: Undebuggable [45] 6 00000001
00:03:13: RADIUS: Service-Type [6] 6 Login
00:03:13: RADIUS: Vendor, Cisco [26] 27 VT=33 TL=21 h323-gw-id=5300_43.
00:03:13: RADIUS: Vendor, Cisco [26] 55 VT=01 TL=49 h323-incoming-conf-id=8F3A3163
B4980003 0 29BD0
00:03:13: RADIUS: Vendor, Cisco [26] 31 VT=26 TL=25 h323-call-origin=answer
00:03:13: RADIUS: Vendor, Cisco [26] 32 VT=27 TL=26 h323-call-type=Telephony
```

```
00:03:13: RADIUS: Vendor, Cisco [26] 57 VT=25 TL=51 h323-setup-time=*16:02:48.681 PST Fri
Dec 31 1999
00:03:13: RADIUS: Vendor, Cisco [26] 59 VT=28 TL=53 h323-connect-time=*16:02:48.946 PST
Fri Dec 31 1999
00:03:13: RADIUS: Vendor, Cisco [26] 62 VT=29 TL=56in=0
00:03:13: RADIUS: Vendor, Cisco [26] 23 VT=01 TL=17 pre-bytes-out=0
00:03:13: RADIUS: Vendor, Cisco [26] 21 VT=01 TL=15 pre-paks-in=0
00:03:13: RADIUS: Vendor, Cisco [26] 22 VT=01 TL=16 pre-paks-out=0
00:03:13: RADIUS: Vendor, Cisco [26] 22 VT=01 TL=16 nas-rx-speed=0
00:03:13: RADIUS: Vendor, Cisco [26] 22 VT=01 TL=16 nas-tx-speed=0
00:03:13: RADIUS: Delay-Time [41] 6 0
00:03:13: RADIUS: Received from id 2 1.7.157.1:1824, Accounting-response, len 20
h323-disconnect-time=*16:03:11.306 PST Fri Dec 31 1999
00:03:13: RADIUS: Vendor, Cisco [26] 32 VT=30 TL=26 h323-disconnect-cause=10
00:03:13: RADIUS: Vendor, Cisco [26] 28 VT=31 TL=22 h323-voice-quality=0
00:03:13: RADIUS: Vendor, Cisco [26] 46 VT=24 TL=40 h323-conf-id=8F3A3163 B4980003 0 29BD0
00:03:13: RADIUS: Acct-Session-Id [44] 10 "00000002"
00:03:13: RADIUS: Acct-Input-Octets [42] 6 0
00:03:13: RADIUS: Acct-Output-Octets [43] 6 88000
00:03:13: RADIUS: Acct-Input-Packets [47] 6 0
00:03:13: RADIUS: Acct-Output-Packets [48] 6 550
00:03:13: RADIUS: Acct-Session-Time [46] 6 22
00:03:13: RADIUS: Vendor, Cisco [26] 30 VT=01 TL=24 subscriber=RegularLine
00:03:13: RADIUS: Vendor, Cisco [26] 35 VT=01 TL=29 h323-ivr-out=Tariff:Unknown
00:03:13: RADIUS: Vendor, Cisco [26] 22 VT=01 TL=16 pre-bytes-
```

The following is sample output from the **debug radius brief** command:

```
Router# debug radius brief
Radius protocol debugging is on
Radius packet hex dump debugging is off
Radius protocol in brief format debugging is on
00:05:21: RADIUS: Initial Transmit ISDN 0:D:23 id 6 10.0.0.1:1824, Accounting-Request, len
358
00:05:21: %ISDN-6-CONNECT: Interface Serial0:22 is now connected to 4085274206
00:05:26: RADIUS: Retransmit id 6
00:05:31: RADIUS: Tried all servers.
00:05:31: RADIUS: No valid server found. Trying any viable server
00:05:31: RADIUS: Tried all servers.
00:05:31: RADIUS: No response for id 7
00:05:31: RADIUS: Initial Transmit ISDN 0:D:23 id 8 10.0.0.0:1823, Access-Request, len 171
00:05:36: RADIUS: Retransmit id 8
00:05:36: RADIUS: Received from id 8 1.7.157.1:1823, Access-Accept, len 115
00:05:47: %ISDN-6-DISCONNECT: Interface Serial0:22 disconnected from 4085274206, call
lasted 26 seconds
00:05:47: RADIUS: Initial Transmit ISDN 0:D:23 id 9 10.0.0.1:1824, Accounting-Request, len
775
00:05:47: RADIUS: Received from id 9 1.7.157.1:1824, Accounting-response, len 20
```

debug tacacs

To display information associated with TACACS, use the **debug tacacs** command in privileged EXEC mode. To disable debugging output, use the no form of this command.

debug tacacs [**accounting | authentication | authorization | events | packet**]

no debug tacacs [**accounting | authentication | authorization | events | packet**]

Syntax Description

accounting	(Optional) TACACS+ protocol accounting.
authentication	(Optional) TACACS+ protocol authentication.
authorization	(Optional) TACACS+ protocol authorization.
events	(Optional) TACACS+ protocol events.
packet	(Optional) TACACS+ packets.

Command Modes

Privileged EXEC

Usage Guidelines

TACACS is a distributed security system that secures networks against unauthorized access. Cisco supports TACACS under the authentication, authorization, and accounting (AAA) security system.

Use the **debug aaa authentication** command to get a high-level view of login activity. When TACACS is used on the router, you can use the **debug tacacs** command for more detailed debugging information.

Examples

The following is sample output from the **debug aaa authentication** command for a TACACS login attempt that was successful. The information indicates that TACACS+ is the authentication method used.

```
Router# debug aaa authentication
14:01:17: AAA/AUTHEN (567936829): Method=TACACS+
14:01:17: TAC+: send AUTHEN/CONT packet
14:01:17: TAC+ (567936829): received authen response status = PASS
14:01:17: AAA/AUTHEN (567936829): status = PASS
```

The following is sample output from the debug tacacs command for a TACACS login attempt that was successful, as indicated by the status PASS:

```
Router# debug tacacs
14:00:09: TAC+: Opening TCP/IP connection to 192.168.60.15 using source 10.116.0.79
14:00:09: TAC+: Sending TCP/IP packet number 383258052-1 to 192.168.60.15 (AUTHEN/START)
14:00:09: TAC+: Receiving TCP/IP packet number 383258052-2 from 192.168.60.15
14:00:09: TAC+ (383258052): received authen response status = GETUSER
14:00:10: TAC+: send AUTHEN/CONT packet
14:00:10: TAC+: Sending TCP/IP packet number 383258052-3 to 192.168.60.15 (AUTHEN/CONT)
14:00:10: TAC+: Receiving TCP/IP packet number 383258052-4 from 192.168.60.15
14:00:10: TAC+ (383258052): received authen response status = GETPASS
14:00:14: TAC+: send AUTHEN/CONT packet
14:00:14: TAC+: Sending TCP/IP packet number 383258052-5 to 192.168.60.15 (AUTHEN/CONT)
14:00:14: TAC+: Receiving TCP/IP packet number 383258052-6 from 192.168.60.15
14:00:14: TAC+ (383258052): received authen response status = PASS
14:00:14: TAC+: Closing TCP/IP connection to 192.168.60.15
```

The following is sample output from the debug tacacs command for a TACACS login attempt that was unsuccessful, as indicated by the status FAIL:

```
Router# debug tacacs
13:53:35: TAC+: Opening TCP/IP connection to 192.168.60.15 using source
192.48.0.79
13:53:35: TAC+: Sending TCP/IP packet number 416942312-1 to 192.168.60.15
(AUTHEN/START)
13:53:35: TAC+: Receiving TCP/IP packet number 416942312-2 from 192.168.60.15
13:53:35: TAC+ (416942312): received authen response status = GETUSER
13:53:37: TAC+: send AUTHEN/CONT packet
13:53:37: TAC+: Sending TCP/IP packet number 416942312-3 to 192.168.60.15
(AUTHEN/CONT)
13:53:37: TAC+: Receiving TCP/IP packet number 416942312-4 from 192.168.60.15
13:53:37: TAC+ (416942312): received authen response status = GETPASS
13:53:38: TAC+: send AUTHEN/CONT packet
13:53:38: TAC+: Sending TCP/IP packet number 416942312-5 to 192.168.60.15
(AUTHEN/CONT)
13:53:38: TAC+: Receiving TCP/IP packet number 416942312-6 from 192.168.60.15
13:53:38: TAC+ (416942312): received authen response status = FAIL
13:53:40: TAC+: Closing TCP/IP connection to 192.168.60.15
```

firewall ip access-group

To specify that the IP firewall is profile-based, use the **firewall ip access-group** command in hotline-rules subcommand configuration mode. Use the **no** form to disable this feature.

firewall ip access-group {*acl-no* | *word*} {**in** | **out**}

no firewall ip access-group {*acl-no* | *word*} {**in** | **out**}

Syntax Description

acl-no	Specifies the ACL number. The ranges are 100-199 and 2000-2699.
word	.
in	.
out	

Defaults

There are no default values.

Command Modes

hotline-rules subcommand mode.

Command History

Release	Modification
12.4(15)XM	This command was introduced.

Usage Guidelines

Examples

The following example illustrates the **firewall ip access-group** command:

```
router (hotline-rules) # firewall ip access-group 199
```

ip local pool

To configure a local pool of IP addresses to be used when a remote peer connects to a point-to-point interface, to generate traps when pool utilization reaches a high or low threshold in percentage, use the **ip local pool** command in global configuration mode. To remove a range of addresses from a pool (the longer of the **no** forms of this command), or to delete an address pool (the shorter of the **no** forms of this command), use one of the **no** forms of this command.

ip local pool {**default** | *poolname*} [*low-ip-address* [*high-ip-address*]] [**group** *group-name*] [**cache-size** *size*] [**priority** *0-255*] [**theshold** *low-threshold high-threshold*]

no ip local pool *poolname low-ip-address* [*high-ip-address*]

no ip local pool {**default** | *poolname*}

Syntax Description

default	Creates a default local IP address pool that is used if no other pool is named.
poolname	Name of the local IP address pool.
low-IP-address [*high-IP-address*]	First and, optionally, last address in an IP address range.
group *group-name*	(Optional) Creates a pool group.
cache-size *size*	(Optional) Sets the number of IP address entries on the free list that the system checks before assigning a new IP address. Returned IP addresses are placed at the end of the free list. Before assigning a new IP address to a user, the system checks the number of entries from the end of the list (as defined by the **cache-size** *size* option) to determine that there are no returned IP addresses for that user. The range for the cache size is 0 to 100. The default cache size is 20.
low-threshold	*low-threshold* is the low threshold configured to generate pool utilization traps. The value of this variable should never be greater than the value the *high threshold.*
high threshold	*high threshold* is the high threshold configured to generate pool utilization traps. The value of this variable should never be less than the value the *lowthreshold.*
priority *0-255*	(Optional) Assigns a priority to the newly created pool, and the same is used to assign an IP address.

Defaults

No address pools are configured. Any pool created without the optional **group** keyword is a member of the base system group.

Command Modes

Global configuration

Command History

Release	Modification
11.0	This command was introduced.
11.3 AA	This command was enhanced to allow address ranges to be added and removed.
12.1(5)DC	This command was enhanced to allow pool groups to be created.

Release	Modification
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T and support was added for the Cisco 6400 node route processor 25v (NRP-25v) and Cisco 7400 platforms.
12.3(14)YX5	The *low-threshold* and *high-threshold* variables were added.

Usage Guidelines

Use the **ip local pool** command to create one or more local address pools from which IP addresses are assigned when a peer connects. You may also add another range of IP addresses to an existing pool. To use a named IP address pool on an interface, use the **peer default ip address pool** interface configuration command. A pool name can also be assigned to a specific user using authentication, authorization, and accounting (AAA) RADIUS and TACACS functions.

If no named local IP address pool is created, a default address pool is used on all point-to-point interfaces after the **ip address-pool local** global configuration command is issued. If no explicit IP address pool is assigned, but pool use is requested by use of the **ip address-pool local** command, the special pool named "default" is used.

The optional **group** keyword and associated group name allows the association of an IP address pool with a named group. Any IP address pool created *without* the **group** keyword automatically becomes a member of a *base* system group.

An IP address pool name can be associated with only one group. Subsequent use of the same pool name, within a pool group, is treated as an extension of that pool, and any attempt to associate an existing local IP address pool name with a different pool group is rejected. Therefore, each use of a pool name is an implicit selection of the associated pool group.

Note To reduce the chances of inadvertent generation of duplicate addresses, the system allows creation of the special pool named "default" only in the base system group, that is, no group name can be specified with the pool name "default."

All IP address pools within a pool group are checked to prevent overlapping addresses; however, no checks are made between any group pool member and a pool not in a group. The specification of a named pool within a pool group allows the existence of overlapping IP addresses with pools in other groups, and with pools in the base system group, but not among pools within a group. Otherwise, processing of the IP address pools is not altered by their membership in a group. In particular, these pool names can be specified in **peer** commands and returned in RADIUS and AAA functions with no special processing.

IP address pools can be associated with Virtual Private Networks (VPNs). This association permits flexible IP address pool specifications that are compatible with a VPN and a VPN routing and forwarding instance (VRF).

The IP address pools can also be used with the **translate** commands for one-step vty-async connections and in certain AAA or TACACS+ authorization functions. Refer to the chapter "Configuring Protocol Translation and Virtual Asynchronous Devices" in the *Cisco IOS Terminal Services Configuration Guide* and the "System Management" part of the *Cisco IOS Configuration Fundamentals Configuration Guide* for more information.

Low and High Thresholds

Cisco Mobile Wireless Home Agent Release 3.1 enhanced the CISCO-IP-LOCAL-POOL-MIB to generate traps when pool utilization reached a low threshold or high threshold in percentage. Objects "cIpLocalPoolPercentAddrThldLo" and "cIpLocalPoolPercentAddrThldHi" are defined for the high and low threshold watermark, respectively.

When the percentage of used addresses in an IP local pool equals or exceeds the high threshold, a "cilpPercentAddrUsedHiNotif" notification is generated. Once the notification is generated, it is disarmed and will not be generated again until the number of used addresses falls below the value indicated by "cIpLocalPoolPercentAddrThldLo".

When the percentage of used addresses in an IP local pool falls below the low threshold, a "cilpPercentAddrUsedLoNotif" notification will be generated. Once the notification is generated, it is disarmed and will not be generated again until the number of used addresses equals or exceeds the value indicated by "cIpLocalPoolPercentAddrThldHi".

IP address pools are displayed with the **show ip local pool** EXEC command.

Examples

The following example creates a pool of local IP addresses named "XYZPool," which contain all IP addresses in the range 100.1.1.1 to 100.1.1.10. The group is named "MWG", and the command specifies a cache size of **50**, and a low and high threshold of **50** and **90**:

```
Router(config)# ip local pool XYZPool  100.1.1.1  100.1.1.10 group MWG cache-size 50
threshold 50 90
```

The following example creates a group of local IP address pools named "pool2," which contains all IP addresses in the range 172.16.23.0 to 172.16.23.255:

```
ip local pool pool2 172.16.23.0 172.16.23.255
```

The following example configures a pool of 1024 IP addresses:

```
no ip local pool default
ip local pool default 10.1.1.0 10.1.4.255
```

Note Although not required, it is good practice to precede local pool definitions with a **no** form of the command to remove any existing pool, because the specification of an existing pool name is taken as a request to extend that pool with the new IP addresses. If the intention is to extend the pool, the **no** form of the command is not applicable.

The following example configures multiple ranges of IP addresses into one pool:

```
ip local pool default 10.1.1.0 10.1.9.255
ip local pool default 10.2.1.0 10.2.9.255
```

The following examples show how to configure two pool groups and IP address pools in the base system group:

```
ip local pool p1_g1 10.1.1.1 10.1.1.50 group grp1
ip local pool p2_g1 10.1.1.100 10.1.1.110 group grp1
ip local pool p1_g2 10.1.1.1 10.1.1.40 group grp2
ip local pool lp1 10.1.1.1 10.1.1.10
ip local pool p3_g1 10.1.2.1 10.1.2.30 group grp1
ip local pool p2_g2 10.1.1.50 10.1.1.70 group grp2
ip local pool lp2 10.1.2.1 10.1.2.10
```

In the example:

- Group grp1 consists of pools p1_g1, p2_g1, and p3_g1.
- Group grp2 consists of pools p1_g2 and p2_g2.
- Pools lp1 and lp2 are not associated with a group and are therefore members of the base system group.

Note that IP address 10.1.1.1 overlaps groups grp1, grp2, and the base system group. Also note that there is no overlap within any group including the base system group, which is unnamed.

The following examples show configurations of IP address pools and groups for use by a VPN and VRF:

```
ip local pool p1_vpn1 10.1.1.1 10.1.1.50 group vpn1
ip local pool p2_vpn1 10.1.1.100 10.1.1.110 group vpn1
ip local pool p1_vpn2 10.1.1.1 10.1.1.40 group vpn2
ip local pool lp1 10.1.1.1 10.1.1.10
ip local pool p3_vpn1 10.1.2.1 10.1.2.30 group vpn1
ip local pool p2_vpn2 10.1.1.50 10.1.1.70 group vpn2
ip local pool lp2 10.1.2.1 10.1.2.10
```

The examples show configuration of two pool groups, including pools in the base system group, as follows:

- Group vpn1 consists of pools p1_vpn1, p2_vpn1, and p3_vpn1.
- Group vpn2 consists of pools p1_vpn2 and p2_vpn2.
- Pools lp1 and lp2 are not associated with a group and are therefore members of the base system group.

Note that IP address 10.1.1.1 overlaps groups vpn1, vpn2, and the base system group. Also note that there is no overlap within any group including the base system group, which is unnamed.

The VPN needs a configuration that selects the proper group by selecting the proper pool based on remote user data. Thus, each user in a given VPN can select an address space using the pool and associated group appropriate for that VPN. Duplicate addresses in other VPNs (other group names) are not a concern, because the address space of a VPN is specific to that VPN.

In the example, a user in group vpn1 is associated with some combination of the pools p1_vpn1, p2_vpn1, and p3_vpn1, and is allocated addresses from that address space. Addresses are returned to the same pool from which they were allocated.

Related Commands

Command	Description
debug ip peer	Displays additional output when IP address pool groups are defined.
ip address-pool	Enables an address pooling mechanism used to supply IP addresses to dial in asynchronous, synchronous, or ISDN point-to-point interfaces.
peer default ip address	Specifies an IP address, an address from a specific IP address pool, or an address from the DHCP mechanism to be returned to a remote peer connecting to this interface.
show ip local pool	Displays statistics for any defined IP address pools.
translate lat	Translates a LAT connection request automatically to another outgoing protocol connection type.
translate tcp	Translates a TCP connection request automatically to another outgoing protocol connection type.

ip mobile cdma ha-chap send attribute

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

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

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

Syntax Description

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

Defaults

There are no default values.

Command Modes

Global configuration

Command History

Release	Modification
12.3(14)YX1	This command was introduced.

Usage Guidelines

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

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

Examples

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

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

ip mobile home-agent

To enable and control Home Agent services on the router, use the **ip mobile home-agent** global configuration command. To disable these services, use the **no** form of this command.

ip mobile home-agent [**home-agent** *address*] [**accounting**] [**broadcast**] [**care-of-access** *acl*] [**dynamic-address**] [**lifetime** *number*] [**aaa | attribute framed-pool**] [**nat-detect**] [**redundancy**] [**reject-static-addr**] [**revocation**] [**replay** *seconds*] [**resync-sa**] [**reverse-tunnel off**] [**roam-access** *acl*] [**hotline profile** *profile-id*] [**strip-realm**] [**suppress-unreachable**] [**local-timezone**] [**nat**] [**unknown-ha** [**accept | deny**]] [**send-mn-address**]

no ip mobile home-agent [**home-agent** *address*] [**accounting**] [**broadcast**] [**care-of-access** *acl*] [**dynamic-address**] [**lifetime** *number*] [**aaa | attribute framed-pool**] [**nat-detect**] [**redundancy**] [**reject-static-addr**] [**revocation**] [**replay** *seconds*] [**resync-sa**] [**reverse-tunnel off**] [**roam-access** *acl*] [**hotline profile** *profile-id*] [**strip-realm**] [**suppress-unreachable**] [**local-timezone**] [**nat**] [**unknown-ha** [**accept | deny**]] [**send-mn-address**]

Syntax Description

home-agent *address*	(Optional) IP address for virtual networks.
accounting	(Optional) Enables Home Agent accounting.
broadcast	(Optional) Enables broadcast datagram routing. By default, broadcasting is disabled.
care-of-access *acl*	(Optional) Controls which care-of addresses (in registration request) are permitted by the Home Agent. By default, all care-of addresses are permitted. The access control list can be a string or number from 1 to 99.
dynamic-address	(Optional) Configures Dynamic HA assignment address.
lifetime *number*	(Optional) Specifies the global registration lifetime for a mobile node. Note that this can be overridden by the individual mobile node configuration. Range is from 3 to 65535 (infinity). Default is 36000 seconds (10 hours). Registrations requesting a lifetime greater than this value will still be accepted, but will use this lifetime value.
aaa	(Optional) Specifies HA AAA access settings.
attribute framed-pool	(Optional) Supports the RADIUS Framed Pool name downloaded during authentication.
redundancy	(Optional) Specifies Home Agent redundancy operation.
reject-static-addr	(Optional) Rejects used Mobile Node Static IP address request.
revocation	(Optional) Enables Registration Revocation.
nat	(Optional) NAT traversal settings.
nat-detect	(Optional) Allows the Home Agent to detect registration requests from a mobile node traversing a NAT-enabled device and apply a tunnel to reach the mobile node. By default, NAT detection is disabled.
replay *seconds*	(Optional) Sets the replay protection time-stamp value. Registration received within this time is valid.
resync-sa	(Optional) Enables resync of security association after failure.
reverse-tunnel-private address	(Optional) Enables support of reverse tunnel by the Home Agent. By default, reverse tunnel support is enabled. Reverse tunneling is mandatory for Private Mobile IP addresses.

roam-access *acl*	(Optional) Controls which mobile nodes are permitted or denied to roam. By default, all specified mobile nodes can roam.
hotline profile *profile-id*	(Optional) Configures profile or rule-based hot-lining for each user (MN). this command acts as sub-configuration mode to configure set of rules. exit Exit from hotline profile configuration mode firewall Firewall Rules no Negate the hotline rules redirect Redirection Rules
strip-nai-realm	(Optional) Strips the realm part of the NAI before authentication is performed.
suppress-unreachable	(Optional) Disables sending ICMP unreachable messages to the source when a mobile node on the virtual network is not registered, or when a packet came in from a tunnel interface created by the Home Agent (in the case of a reverse tunnel). By default, ICMP unreachable messages are sent.
local-timezone	(Optional) Adjusts the UTC time based on the local time zone configured and uses the adjusted time for proxy mobile IP registration.
unknown-ha [**accept** | **deny**]	When **unknown-ha accept** is configured, the Home Agent will accept the Mobile IP Registration request with Home Agent address different unicast from the IP destination of the Mobile IP registration request, and the Home Agent address set in the Registration Reply is that of the IP destination address. When **unknown-ha deny** is configured, the Home Agent will deny the the Mobile IP Registration request with Home Agent address different unicast from the IP destination of the Mobile IP registration request with Error Code Unknown HomeAgent, and the Homeagent address set in the Reject Registration Reply is that of the IP destination address.
send-mn-address	Sends home address (as received in mobile IP registration request) in Access Request messages forHA-CHAP. **Note** You must configure this keyword in the Home Agent to send **radius-server vsa send authentication 3gpp2** attributes.

Defaults

This command is disabled by default. Broadcasting is disabled by default. Reverse tunnel support is enabled by default. ICMP Unreachable messages are sent by default.

Command Modes

Global configuration

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2(2)XC	The **strip-nai-realm** and **local-timezone** keywords were added.
12.2(8)ZB6	The **unknown** [**accept** | **deny**] and **send-mn-address** keywords were added.
12.3(14)YX	The **accounting**, **dynamic-address**, **redundancy**, **reject-static-addr,** and **resync-sa** keywords were added.

Release	Modification
12.4(15)XL	The **attribute framed-pool** keyword was added.
12.4(15)XM	The **hotline profile** keyword was added.

Usage Guidelines

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

The Home Agent is responsible for processing registration requests from the mobile node and setting up tunnels and routes to the care-of address. Packets to the mobile node are forwarded to the visited network.

The Home Agent will forward broadcast packets to mobile nodes if they registered with the service. However, heavy broadcast traffic utilizes the CPU of the router. The Home Agent can control where the mobile nodes roam by the **care-of-access** parameter, and which mobile node is allowed to roam by the **roam-access** parameter.

When a registration request comes in, the Home Agent will ignore requests when Home Agent service is not enabled or the security association of the mobile node is not configured. The latter condition occurs because the security association must be available for the MH authentication extension in the reply. If a security association exists for the Foreign Agent (IP source address or care-of address in request), the Foreign Agent is authenticated, and then the mobile node is authenticated. The Identification field is verified to protect against replay attack. The Home Agent checks the validity of the request (see Table 5) and sends a reply. (Replay codes are listed in Table 6.) A security violation is logged when Foreign Agent authentication, MH authentication, or Identification verification fails. (The violation reasons are listed in Table 7.)

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

By default, the HA uses the entire NAI string as username for authentication (which may be with local security association or retrieved from the AAA server). The **strip-nai-realm** parameter instructs the HA to strip off the realm part of NAI (if it exists) before performing authentication. Basically, the mobile station is identified by only the username part of NAI.

When the packet destined for the mobile node arrives on the Home Agent, the Home Agent encapsulates the packet and tunnels it to the care-of address. If the Don't fragment bit is set in the packet, the outer bit of the IP header is also set. This allows the Path MTU Discovery to set the MTU of the tunnel. Subsequent packets greater than the MTU of the tunnel will be dropped and an ICMP datagram too big message sent to the source. If the Home Agent loses the route to the tunnel endpoint, the host route to the mobile node will be removed from the routing table until tunnel route is available. Packets destined for the mobile node without a host route will be sent out the interface (home link) or to the virtual network (see the description of **suppress-unreachable** keyword). For subnet-directed broadcasts to the home link, the Home Agent will send a copy to all mobile nodes registered with the broadcast routing option.

Table 5 describes how the Home Agent treats registrations with various bits set when authentication and identification are passed.

Table 5 Home Agent Registration Bitflags

Bit Set	Registration Reply
S	Accept with code 1 (no simultaneous binding).
B	Accept. Broadcast can be enabled or disabled.
D	Accept. Tunnel endpoint is a collocated care-of address.
M	Deny. Minimum IP encapsulation is not supported.
G	Accept. GRE encapsulation is supported.
V	Ignore. Van Jacobsen Header compression is not supported.
T	Accept if **reverse-tunnel-off** parameter is not set.
reserved	Deny. Reserved bit must not be set.

Table 6 lists the Home Agent registration reply codes.

Table 6 Home Agent Registration Reply Codes

Code	Reason
0	Accept.
1	Accept, no simultaneous bindings.
128	Reason unspecified.
129	Administratively prohibited.
130	Insufficient resource.
131	Mobile node failed authentication.
132	Foreign agent failed authentication.
133	Registration identification mismatched.
134	Poorly formed request.
136	Unknown Home Agent address.
137	Reverse tunnel is unavailable.
139	Unsupported encapsulation.

Table 7 lists security violation codes.

Table 7 Security Violation Codes

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

Examples

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

```
ip mobile home-agent ?
    aaa HA AAA access settings
    accounting Enable Home Agent accounting
    address HA address for virtual networks
    broadcast Enable forwarding of broadcast packets
    care-of-access Care-of roaming capability access-list
    dynamic-address Configure Dynamic HA assignment address
    lifetime Global lifetime for mobile hosts
    local-timezone Use Local Time Zone to generate Identification Fields
    nat NAT traversal settings
    nat-detect Enable NAT detect on Home Agent
    redundancy Home Agent redundancy operation
    reject-static-addr Reject Used Mobile Node Static IP Addr Request
    replay Set replay protection timestamp value for all SAs
    resync-sa Turn on resync of SA after failure
    reverse-tunnel Reverse Tunneling for Mobile IP
    revocation Enable Registration Revocation
    roam-access Mobile host roaming capability access-list
    send-mn-address Send MN address as Framed-IP-Address in HA-CHAP
    strip-realm Strip off NAI realm part
    suppress-unreachable Disable sending ICMP unreachable
    template Configure a tunnel template for tunnels to the Home Agent
    unknown-ha Unknown HA address in registration request
```

Here is an example of the framed-pool attribute:

```
ip mobile home-agent aaa attribute Framed-Pool
ip local pool haPool 70.1.1.1 70.1.1.254
ip mobile home-agent
ip mobile virtual-network 70.1.1.0 255.255.255.0
ip mobile host nai @cisco.com interface FastEthernet1/0 aaa load-sa
```

Related Commands

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

ip mobile home-agent accounting

To enable the Home Agent accounting feature, use the **ip mobile home-agent accounting** command in global configuration mode.

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

Syntax Description

method name	Specifies the named accounting list used to generate accouting records. The accounting method is configured using the **aaa accounting network** command.
default	Specifies the default accounting list.

Defaults

There are no default values for this command.

Command Modes

Global configuration

Command History

Release	Modification
12.2(8)ZB7	This command was introduced.

Usage Guidelines

The Home Agent cannot open more than 100k bindings if HA Accounting feature is enabled.

Examples

The following example illustrates the **ip mobile home-agent accounting** command:

```
Router# ip mobile home-agent accounting method name
```

ip mobile home-agent debug include username

To display the username or IMSI condition with each debug statement, use the **ip mobile home-agent debug include username** command. To disable this function, use the **no** form of the command.

ip mobile home-agent debug include username

no ip mobile home-agent debug include username

Syntax Description

There are no keywords or arguments for this command.

Defaults

There are no default values for this command.

Command Modes

Global configuration

Command History

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

Usage Guidelines

The following example illustrates the **ip mobile home-agent debug include username** command:

```
Router# ip mobile home-agent debug include username
```

ip mobile home-agent dfp-max-weight

To configure the maximum dfp weight that is allowed on the HA, use the **ip mobile home-agent dfp-max-weight** command in global configuration mode. Use the **no** form of the command to disable this feature.

ip mobile home-agent dfp-max-weight *dfp-max-weight-value*

no ip mobile home-agent dfp-max-weight

Syntax Description

dfp-max-weight-value	The maximum dfp weight that is allowed on the HA. The default value is 24.

Defaults

The *dfp-max-weight-value* is 24.

Command Modes

Global configuration

Command History

Release	Modification
12.4(15)XM	This command was introduced.

Examples

The following example illustrates the **ip mobile home-agent dfp-max-weight** command:

```
Router(config)# ip mobile home-agent 24
```

ip mobile home-agent dynamic-address

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

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

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

Syntax Description

ip address	The IP address of the Home Agent.

Defaults

The Home Agent Address field will be set to *ip address.*

Command Modes

Global configuration

Command History

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

Examples

The following example illustrates the **ip mobile home-agent dynamic address** command:

```
Router# ip mobile home-agent dynamic address 1.1.1.1
```

ip mobile home-agent host-config url

To configure a URLon the HA that allows the MN to download configuration parameters, use the **ip mobile home-agent host-config** url command in globabl configuration mode. Use the no form of the command to disable the feature.

ip mobile home-agent host-config *url*

no ip mobile home-agent host-config *url*

Syntax Description

url	The generic *url* that you can specify that allows the MN to download its configuration parameters.

Defaults

This command is disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.4(15)XM	This command was introduced.

Usage Guidelines

This command is necessary because sometimes the HA is not able to provide the configuration requested by the MN. This command configures a generic site specified by the URL that helps the MN to download its configuration parameters.

Examples

The following example illustrates the **ip mobile home-agent host-config** command:

```
Router(config)# ip mobile home-agent host-config http://www.cisco.com
```

ip mobile home-agent hotline

To distinguish Profile or Rule based hot-lining for each user (MN), and to enter the hotline-rules sub configuration mode, use the **ip mobile home-agent hotline** command in global configuration mode. Use the **no** form of the command to disable this feature.

ip mobile home-agent hotline [profile *word***]**

no ip mobile home-agent hotline [profile *word***]**

Syntax Description

profile *word*	(Optional) Denotes whether hotlining will be profile based, or rule based. If not configured, hotlining will be rule based.

Defaults

The default value is rule based hotlining.

Command Modes

Global configuration

Command History

Release	Modification
12.4(15)XM	This command was introduced.

Examples

The following example illustrates the **ip mobile home-agent hotline** command:

```
Router(config)# [no] ip mobile home-agent hotline profile word
Router(hotline-rules)#

Router(hotline-rules)#?
  exit      Exit from hotline profile configuration mode
  firewall  Firewall Rules
  no        Negate the hotline rules
  redirect  Redirection Rules
```

ip mobile home-agent max-binding

To limit the number of bindings that can be opened on the HA, use the **ip mobile home-agent max-binding** command in global configuration mode. Use the **no** form of the command to disable the feature.

ip mobile home-agent max-binding *max-binding value*

no ip mobile home-agent max-binding *max-binding value*

Syntax Description

max-binding value	Limits the number of bindings that can be opened on the HA.

Defaults

The default value of max-binding-value is 235,000. When Accounting is enabled the supported value is 150,000.

Command Modes

Global configuration

Command History

Release	Modification
12.4(15)XM	This command was introduced.

Examples

The following example illustrates the **ip mobile home-agent max-binding** command:

```
Router# ip mobile home-agent max-binding 235000
```

ip mobile home-agent max-cps

To configure the maximum cps that is allowed on the HA, use the **ip mobile home-agent max-cps** command in global configuration mode. Use the **no** form of the command to disable this feature.

ip mobile home-agent max-cps *max-cps-value*

no ip mobile home-agent max-cps

Syntax Description

max-cps-value	The maximum cps value that is allowed on the HA. The default value is 160cps with accounting support.

Defaults

The default value is 160cps with accounting support.

Command Modes

Global configuration

Command History

Release	Modification
12.4(15)XM	This command was introduced.

Examples

The following example illustrates the **ip mobile home-agent max-cps** command:

```
Router(config)# ip mobile home-agent max-cps 160
```

ip mobile home-agent redundancy

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

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

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

Syntax Description

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

Defaults

No global Home Agent addresses are specified.

Command Modes

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

Command History

Release	Modification
12.0(2)T	This command was introduced.
12.3(7)XJ1	The **mode active-standby** option was added.

Usage Guidelines

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

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

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

When Mobile IP standby is configured, the Home Agent can request mobility bindings from the peer Home Agent. When the command is deconfigured, the Home Agent can remove mobility bindings. The following describes how Home Agent redundancy operates on physical and virtual networks.

Physical network:

Only the active Home Agent will receive registrations. It updates the standby Home Agent. The standby Home Agent requests the mobility binding table from the active Home Agent. When Mobile IP standby is deconfigured, the standby Home Agent removes all bindings, but the active Home Agent keeps all bindings.

Virtual network:

Both active and standby Home Agents receive registrations if the loopback interface is used; each will update the peer after accepting a registration. Otherwise, the active Home Agent receives registrations. Both active and standby Home Agents request mobility binding tables from each other. When Mobile IP standby is deconfigured, the standby or active Home Agent removes all bindings.

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

Examples

The following is sample output from the **ip mobile home-agent redundancy** command that specifies an HSRP group name of SanJoseHA:

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

ip mobile home-agent redundancy periodic-sync

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

ip mobile home-agent *method* **redundancy [virtual-network address** *address*] **periodic-sync**

no ip mobile home-agent *method* **redundancy [virtual-network address** *address*] **periodic-sync**

Syntax Description

method name	Specifies the named accounting list used to generate accouting records. The accounting method is configured using the **aaa accounting network** command.
virtual-network	(Optional) Specifies that the HSRP group is used to support virtual networks.
address *addr*	(Optional) Home agent address.

Defaults

There are no default values for this command.

Command Modes

Global configuration

Command History

Release	Modification
12.x(14)YX	This command was introduced.

Usage Guidelines

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

Examples

The following example illustrates the **ip mobile home-agent redundancy periodic-sync** command:

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

ip mobile home-agent reject-static-addr

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

ip mobile home-agent reject-static-addr

Syntax Description

This command has not arguments or keywords

Command Modes

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

Command History

Release	Modification
12.2(8)BY	This command was introduced.

Usage Guidelines

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

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

Examples

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

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

ip mobile home-agent resync-sa

To configure the HA to clear out the old cached security associations and requery the AAA server, use the **ip mobile home-agent resync-sa** command global configuration command.

ip mobile home-agent resync-sa *x*

Syntax Description

x	Specifies the time that the HA will use to initiate a resync.

Command Modes

Global configuration.

Command History

Release	Modification
12.1	This command was introduced.

Usage Guidelines

When a MN tries to reregister with the HA, the time change from the original timestamp is checked. If that time period is less than x, and the MN fails authentication, then the HA will not requery the AAA server for another SA.

If the MN reregisters with the HA, and the time between registrations is greater than x, and the MN fails registrations, then the HA will clear out the old SA and requery the AAA server.

Examples

The following example illustrates the **ip mobile home-agent resync-sa** command:

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

ip mobile home-agent revocation

To enable support for MIPv4 Registration Revocation on the HA, use the **ip mobile home-agent revocation** command in global configuration mode. Use the **no** form of the command to disable this feature.

ip mobile home-agent revocation [timeout *1-100***] [retransmit** *0-100***] [timestamp msec]**

no ip mobile home-agent revocation [timeout *1-100***] [retransmit** *0-100***] [timestamp msec]**

Syntax Description

timeout *1-100*	(Optional) Configures the time interval (in seconds) between re-transmission of MIPv4 Registration Revocation Message. The **no** version restores the time interval between re-transmission of MIPv4 Registration Revocation Message to the default value. The default is **5** seconds.
retransmit *0-100*	(Optional) Configures number of times MIPv4 Registration Revocation messages are retransmitted. The **no** version of this command restores the retransmit number to the default value. The default is **3** re-transmissions.
timestamp msec	(Optional) Configures the units in which the timestamp value in the revocation support extension and revocation message should be encoded. By default the timestamp value will be sent as seconds. If **msec** option is specified, the values will be encoded in milliseconds

Defaults

The **timeout** default setting is **5** seconds, the **retransmit** default setting is **3** retransmissions, and the default **timestamp** setting is seconds.

Command Modes

Global configuration.

Command History

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

Examples

The following example illustrates the **ip mobile home-agent revocation** command:

```
Router# (config)#ip mobile home-agent revoc timeout ?
  <1-100>  Wait time (default 3 secs)
Router# (config)#ip mobile home-agent revoc retransmit ?
  <0-100>  Number of retries for a transaction (default 3)
```

ip mobile home-agent revocation ignore

To enable the HA to send a revocation acknowledgement to the PDSN/FA but not delete the binding, use the **ip mobile home-agent revocation ignore** command in global configuration mode. Use the **no** form of the command to disable this function.

ip mobile home-agent revocation ignore *fa acl*

no ip mobile home-agent revocation ignore *fa acl*

Syntax Description

fa-acl	Specifies either an acl number *1-99*, or a name.

Defaults

There are no default values.

Command Modes

Global configuration.

Command History

Release	Modification
12.3(14)YX5	This command was introduced.

Usage Guidelines

When a subscriber roams between their service provider's network and another partner service provider's network, the PDSN gateway sends a Resource Revocation message to the Home Agent to remove the subscriber. This causes timing problems, so Selective FA Revocation selectively ignores these "remove subscriber" requests. Revocation is done on a Foreign Agent basis. Thus, a given HA will statically configure a list of Foreign Agents from which to ignore the "remove subscriber" messages.With Selectable FA Revocation, the Hybrid PDSN/FA will go through the above conditions and send the revocation to the Home Agent. However, in this case the HA ignores the revocation, but sends a RR response to the PDSN.

As a result, the MN and Home Agent still have a binding state but the PDSN/FA no longer has a PPP session/visitor table entry. Eventually, the mobile goes active and has Data Ready to Send, where the 1x RF channel **DRS=1** is included. In this scenario, the VLR is not queried and the OpenRP message to the PDSN has **MEI** set to 1. Regardless of the MEI value, the PDSN will initiate PPP, and send a RRQ with the previously assigned home address. In this case HA will accept the Re-registration.

Note **ip mobile home-agent revocation ignore** currently does not support using *1300-1999* (Standard IP access-list number (expanded range).

Examples

Here is an example of the **ip mobile home-agent revocation ignore** command:

You can ignore revocation from the FA by specifying the **standard** access-list number or **standard** access-list name.

Configuring access-list name to ignore the requests from COA 5.1.1.4

```
Router(config)#ip access-list standard ?
  <1-99>       Standard IP access-list number
  <1300-1999>  Standard IP access-list number (expanded range)
  WORD         Access-list name
Router(config)#ip access-list standard fa_acl1
Router(config-std-nacl)#permit 5.1.1.4
```

Configuring access-list number to ignore the requests from COA 5.1.1.5

```
Router(config)#ip access-list standard ?
  <1-99>       Standard IP access-list number
  <1300-1999>  Standard IP access-list number (expanded range)
  WORD         Access-list name
Router(config)#ip access-list standard 1
Router(config-std-nacl)#permit 5.1.1.5
```

Configuring access-list name to selectively ignore requests from FA 5.1.1.4 . This is to associate the above created acl with the **ip mobile home-agent revocation ignore** command.

```
Router((config)#ip mobile home-agent revocation ignore ?
  <1-99>  fa Access-list number
  WORD    fa Access-list name
Router(config)#ip mobile home-agent revocation ignore fa_acl1
```

Configuring the access-list number to selectively ignore requests from FA 5.1.1.5

```
Router(config)#ip mobile home-agent revocation ignore 1
```

ip mobile home-agent service-policy

To attach the HA to the QoS police function, and identify the HA by associating a service-policy to the HA virtual interface object, use the **ip mobile home-agent service-policy** command in global configuration mode. The command is configured for both traffic directions. Use the **no** form of the command to disable this feature.

ip mobile home-agent service-policy [**input** *policy-name*] [**output** *policy-name*]

no ip mobile home-agent service-policy [**input** *policy-name*] [**output** *policy-name*]

Syntax Description

input *policy-name*	Specifies the .
output *policy-name*	Specifies the .

Defaults

The Home Agent Address field will be set to *ip address.*

Command Modes

Global configuration

Command History

Release	Modification
12.4(15)XM	This command was introduced.

Examples

The following example illustrates the **ip mobile home-agent dynamic address** command:

```
Router(config)# ip mobile home-agent service-policy input policy-mip-flow
output policy-mip-flow
```

ip mobile home-agent template tunnel

To configure a Home Agent to use the template tunne, use the **ip mobile home-agent template tunnel** command in global configuration. Use the **no** form to disable this feature.

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

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

Syntax Description

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

Defaults

There are no default values.

Command Modes

Global configuration.

Command History

Release	Modification
12.3(8)XJW	This command was introduced.

Examples

The following example illustrates the **ip mobile home-agent template tunnel** command:

```
Router(config)# interface tunnel 10
     ip access-group 150 in -------> apply access-list 150
Router (config)# access-list 150 deny any  10.10.0.0 0.255.255.255
    access-list permit any any
              ------> permit all but traffic to 10.10.0.0 network
Router (config)# ip mobile home-agent template tunnel 10  address 10.0.0.1
```

ip mobile host

To configure the mobile host or mobile node group, use the **ip mobile host** global configuration command. For PDSN, use this command to configure the static IP address or address pool for multiple flows with the same NAI.

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

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

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	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 or more IP addresses to be assigned using the **static-address** keyword.
local-pool *name*	Name of the local pool of addresses to use for assigning a static IP address to this NAI.
address	Indicates that a dynamic IP address is to be assigned to the flows on this NAI.
addr	IP address to be assigned using the **address** keyword.
pool	Indicates that pool of addresses is to be used in assigning a dynamic IP address.
local *name*	The name of the local pool to use in assigning addresses.
vpdn-tunnel	Mandatory configuration to bring up MIP-LAC tunnel. Indicates that the address for the mobile IP client needs to be obtained from the LNS server using the MIP-LAC feature.
dhcp-proxy-client	Indicates that the pool should come from a DHCP client.
dhcp-server *addr*	IP address of the DHCP server.
interface *name*	Mobile node that belongs to the specified interface. When used with DHCP, this specifies the address pool 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.
skip chap	When **skip-chap** is configured, the Home Agent does not send Access Request to AAA for mobile IP registration requests.

aaa	(Optional) Retrieves security associations from a AAA (TACACS+ or RADIUS) server.
load-sa	(Optional) Stores security associations in memory after retrieval.
permanent	(Optional) Caches security associations in memory after retrieval permanently. Use this optional keyword only for NAI hosts.
authorized-pool *pool*	Verifies the IP address assigned to the mobile if it is within the pool specified by *pname*.
skip-aaa-reauthentication	When configured, the Home Agent does not send Access Request for authentication for mobile IP re-registration requests. When disabled, the Home agent sends Access Request for all mobile IPregistration requests.
care-of-access *acl*	(Optional) Access list. This can be a string or number from 1 to 99. Controls where mobile nodes roam—the acceptable care-of addresses.
lifetime *number*	(Optional) Lifetime (in seconds). The lifetime for each mobile node (group) can be set to override the global value. Possible values are 3 through 65535.

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(8)ZB6	The **skip-aaa-reauthentication** and **authorized-pool** keywords were added.
12.4(15)XM	The **vpdn-tunnel** keyword was introduced.

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 (using 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 an AAA server. When using an AAA server, the router will attempt to download all security associations when the command is entered. If no security associations are retrieved, retrieval will be attempted when a registration request arrives or the **clear ip mobile secure** command is entered.

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 8 are based on the assumption of one security association per mobile node.

The **nai** keyword allows you to specify a particular mobile station or range of mobile stations. The mobile station 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). Or, the mobile station 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 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 **vpdn-tunnel** option is added to the **ip mobile host** command. This keyword is mandatory to bring up MIP-LAC tunnel. You must also configure the **vpdn-tunnel virtual-template** option of the **ip mobile realm** command to enable the MIP-LAC feature. Every MIP session matching this realm will be mapped to a corresponding L2TP session. When MIP-LAC is enabled for user(s), and the HA does not go to AAA for authentication / authorization, local configuration will be checked for VPDN parameters.

The address pool can be defined by a local pool or using a DHCP proxy client. For DHCP, the **interface** *name* specifies the address pool from which the DHCP server selects and **dhcp-server** specifies DHCP server address.

Security associations can be stored using one of three methods:

- On the router
- On the AAA server, retrieve security association each time registration comes in
- On the AAA server, retrieve and store security association

Each method has advantages and disadvantages, which are described in Table 8

.

Table 8 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 only need memory to load in a security association, and then release the memory when done. Router can support unlimited number of mobile nodes.	• 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 8 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.

Note With **load-sa**, the security association downloaded from AAA will be cached and stored in the HA so that no RADIUS requests are needed to download a security association for a mobile for renewal. To avoid going to AAA for authentication when mobile ip re-registration message (RRQ) is received, or during closure of session when RRQ(0) is received, use the **skip-aaa-reauthentication** option.

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 store its security associations on the AAA server:

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

The following example configures a local pool of dynamic addresses to be used in assigning IP addresses to mobile stations 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 65535
```

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

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

Related Commands

Command	Description
aaa authorization ipmobile	Authorizes Mobile IP to retrieve security associations from the AAA server using TACACS+ or RADIUS.
ip mobile secure	Specifies the mobility security associations for mobile host, visitor, Home Agent, and Foreign Agent.
show ip mobile host	Displays mobile station counters and information.
ip mobile proxy-host	Configures the proxy Mobile IP attributes of the PDSN.

ip mobile radius disconnect

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

ip mobile radius disconnect

no ip mobile radius disconnect

Syntax Description

There are no arguments or keywords for this command.

Defaults

The default setting is that there is no processing of Radius Disconnect messages.

Command Modes

Global configuration.

Command History

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

Usage Guidelines

Note In order for POD requests to be processed by AAA, you need to configure the **aaa server radius dynamic-author** command.

Note You must configure **radius-server attribute 32 include-in-access-req** for the HA to send the FQDN in Access Request

Examples

The following example illustrates the **ip mobile radius disconnect** command:

```
Router# ip mobile radius disconnect
```

ip mobile realm

To enable inbound user sessions to be disconnected when specific session attributes are presented, and to configure policy parameters on the Home Agent and attach/identify them to QoS through an APN interface, use the **ip mobile realm** command in global configuration mode. Use the **no** form of the command to disable this feature.

ip mobile realm {*realm* | *nai*} **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 [capability profile-based redirec**t [**ip** | **http**] | **rule-based** *flag*]] [**vpdn-tunnel virtual-template** *number* [**setup-time** *number*]] [**service-policy** {**input** *policy-name* [**peak-rate** *rate*] | **output** *policy-name* [**peak-rate** *rate*]}] [**any-traffic | next-hop** *next-hop-ipadress*]

no ip mobile realm ip mobile realm {*realm* | *nai*} **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 [capability [all** | **httpredir** | **ipfilter** | **ipredir** | **profile**] **redirec**t [**ip** | **http**] | **rule-based** *flag*]] [**vpdn-tunnel virtual-template** *number* [**setup-time** *number*]] [**service-policy** {**input** *policy-name* [**peak-rate** *rate*] | **output** *policy-name* [**peak-rate** *rate*]}] [**any-traffic | next-hop** *next-hop-ipadress*]

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.
capability profile-based redirect ip	(Optional) Configures a profile-based hot-lining for users with ip-redirection rules. Here, the realm can be nai/realm. **all** Support all Hotline Capabilities **httpredir** HTTPRedir Rule-based Hot-Lining **ipfilter** IPFilter Rule-based Hot-Lining **ipredir** IPRedir Rule-based Hot-Lining **profile** Profile-based Hot-Lining
capability profile-based redirect http	(Optional) Configures a profile-based hot-lining for users with http-redirection rules. Here, the realm can be nai/realm.

rule-based *flag*	(Optional) Configures rule-based hot-lining for users. Here, the realm can be nai/realm.
vpdn-tunnel virtual-template *number*	(Optional) Enables you to configure the vpdn-tunnel virtual-template number.
setup-time *number*	(Optional) Enables you to configure the setup time. The range of values for "setup-time" is from 5 secs to 300 secs. The default value for **setup-time** will be 60 seconds. The default value will be taken in to consideration, when you do not specify the **setup-time** option explicitly.
service-policy	(Optional) Configures a policy and associated rate for one or more user bindings belonging to that policy on the basis of NAI/realm.
input *policy-name* [**peak-rate** *rate*]	Attaches the policy-map in input direction (downstream). The **peak-rate** is the police rate value in bps. The range is 8000-2000000000.
output *policy-name* [**peak-rate** *rate*]}]	Attaches a policy-map in output direction (upstream). The **peak-rate** is the police rate value in bps. The range is 8000-2000000000.
any-traffic next-hop *next-hop-ipadress*	Sets the next-hop address for the realm. **any-traffic** indicates that any or all traffic in the upstream from the mobile is redirected. **next-hop** indicates the next-hop feature. *next-hop-ip-address* is the IP address of the next-hop, where the packets needs to be redirected to.

Defaults

When the **setup-time** is not specified, the default value is 60.

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(15)XM	The **capability, redirect** [**ip**	**http**], **rule-based** *flag,* **vpdn-tunnel virtual-template** and **setup-time,** and **service policy**, **input**, **output**, **peak-rate,** and **any traffic next hop** options were introduced.

Usage Guidelines

This command 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. 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 AAA accounting server group is defined, all accounting records for the users of the realm will be sent to the specified group. If AAA authentication server group is defined, HA-CHAP is sent to the server(s) defined in the group.

The *word* argument should be specified as nai/realm and in the format of @cisco.com/username@cisco.com. Otherwise, the command will give error message. At least one form of hot-lining should be selected. There is no default rule to activate rule-based hot-lining for the user. Un-configuring this CLI will erase the rule-based hot-lining capability for the user. The values in above command are mentioned as flags. The flag values are explained here:

0x00000001 Profile-based Hot-Lining is supported (Using RADIUS Filter-Id attributes)
0x00000002 Rule-based Hot-Lining is supported using Filter Rule
0x00000004 Rule-based Hot-Lining is supported using HTTP Redirection Rule.
0x00000008 Rule-based Hot-Lining is supported using IP Redirection Rule.

The [**service-policy** {**input** *policy-name* [**peak-rate** *rate*] | **output** *policy-name* [**peak-rate** *rate*]}] variables allows you to configure a policy and associated rate for one or more user bindings belonging to that policy on the basis of NAI/realm. This can be configured for both upstream and downstream traffic. The burst and the peak-burst can be configured under the policy-map configuration.

The **setup-time** for the **vpdn-tunnel** configuration is optional. The range of values for **setup-time** is from 5 secs to 300 secs. The default value for setup-time is 60 seconds. The default value is taken in to consideration, when user does not specify the **setup-time** option explicitly.

Configured **setup-time** is the maximum tolerance time, starting from the creation of the PPP IDB within which a regenerated PPP session has to come fully up. If this period of time has elapsed and the L2TP tunnel is not up yet, the mobile IP module proceeds to tear down this session's L2TP session, PPP IDB and mobile binding. Also, please note that the *number* option of **tunnel vtemplate** *number* must match the number configured in the corresponding **interface virtual-template** command.

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

Router(config)#ip mobile realm {realm | nai}  hotline ?
  capability  Hotlining Capability of the mobile hosts
  redirect    Redirect ip address for upstream traffic

Router(config)#[no] ip mobile realm {realm | nai} hotline capability ?
  all         Support all Hotline Capabilities
  httpredir   HTTPRedir Rule-based Hot-Lining
  ipfilter    IPFilter Rule-based Hot-Lining
  ipredir     IPRedir Rule-based Hot-Lining
  profile     Profile-based Hot-Lining
Router(config)#
```

Here is a policy map configuration example:

```
Router(config)#ip mobile realm <nai | realm> ?
  dns       Configure DNS details
  hotline   Hotlining of the mobile hosts
  service-policy QoS service policy attachment
  vrf       VRF for the realm
```

```
Router(config)#ip mobile realm <nai | realm> service-policy ?
   input    Attach policy-map in input direction (downstream)
   output  Attach policy-map in output direction (upstream)
   <cr>

Router(config)#ip mobile realm <nai | realm> service-policy input ?
   WORD  Policy-map name in input direction

Router(config)#ip mobile realm <nai | realm> service-policy input <policyname> ?
    output       Attach policy-map in output direction (upstream)
    peak-rate    Police rate
    <cr>

Router(config)#ip mobile realm <nai | realm> service-policy input <policyname> peak-rate ?
    <8000-2000000000>  Police rate value in bps

Router(config)#ip mobile realm <nai | realm> service-policy input <policyname>  peak-rate
<rate> ?
    output       Attach policy-map in output direction (upstream)
    <cr>

Router(config)#ip mobile realm <nai | realm> service-policy input <policyname> peak-rate
<rate> output ?
    WORD  Policy-map name in output direction

Router(config)#ip mobile realm <nai | realm> service-policy input <policyname> peak-rate
<rate> output <policyname> ?
    peak-rate   Police rate

Router(config)#ip mobile realm <nai | realm> service-policy input <policyname> peak-rate
<rate> output <policyname> peak-rate ?
    <8000-2000000000>  Police rate value in bps

Router(config)#ip mobile realm <nai | realm> service-policy input <policyname> peak-rate
<rate> output <policyname> peak-rate <rate>
```

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** global configuration command. To remove the mobility security associations, use the **no** form of this command.

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

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

Syntax Description

host	Security association of the mobile host on the Home Agent.
lower address	IP address of host, visitor, or mobility agent, or lower range of IP address pool.
upper-address	(Optional) Upper range of IP address pool.
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.
address	IP address of visitor or mobility agent.
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 or hexadecimal string of values. No spaces are allowed.
replay	(Optional) Replay protection used on registration packets.
timestamp	(Optional) Used to validate incoming packets to ensure that they are not being “replayed” by a spoofer using timestamp method.
number	(Optional) Number of seconds. Registration is valid if received within the specified time. 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.
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.

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.

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 the mobile node can reregister with the time-stamp value closer to that of the Home Agent, if desired.

Note NTP can be used to synchronize time for all parties.

Examples The following example shows mobile node 20.0.0.1, which has a key that is generated by the MD5 hash of the string:

```
Router# ip mobile secure host 20.0.0.1 spi 100 key hex 12345678123456781234567812345678
```

Related Commands

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

ip mobile tunnel

To specify the settings of tunnels created by Mobile IP, use the **ip mobile tunnel** interface configuration command.

ip mobile tunnel {**crypto map** *map-name* | **route-cache** | **path-mtu-discovery** | **nat** {**inside** | **outside**}}

Syntax Description

crypto map	Enables encryption/decryption on new tunnels.
map-name	Specifies the name of the crypto map.
route-cache	Sets tunnels to default or process switching mode.
path-mtu-discovery	Specifies when the tunnel MTU should expire if set by Path MTU Discovery.
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.

Defaults

Disabled.

Command Modes

Interface configuration.

Command History

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

Usage Guidelines

Path MTU discovery is used by end stations to find a packet size that does not need fragmentation between them. Tunnels have to adjust their MTU to the smallest MTU interior to achieve this. This is described in RFC 2003.

The discovered tunnel MTU should be aged out periodically to possibly recover from case where sub-optimum MTU existed at time of discovery. It is reset to the outgoing interface's MTU.

Examples

The following example sets the discovered tunnel MTU to expire in ten minutes:

```
Router# ip mobile tunnel reset-mtu-time 600
```

ip mobile virtual-network

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

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

no ip mobile virtual-network *net mask* **[address** ***addr*****]**

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 *addr*	(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 was 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 HA IP address is configured on the loopback interface for that virtual network:

```
Router# ip mobile virtual-network

int e0
 ip addr 1.0.0.1 255.0.0.0
 standby ip 1.0.0.10
 standby name SanJoseHA

int lo0
 ip addr 20.0.0.1 255.255.255.255

ip mobile home-agent
 ip mobile virtual-network 20.0.0.0 255.255.0.0 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
```

match flow mip-bind

To classify packets for each binding that belong to a class of MN users with a specified rate, use the **match flow mip-bind** command in MQC class-map config mode. Use the **no** form of the command to delete the classification.

match flow mip-bind

no match flow mip-bind

Syntax Description

There are no keywords or arguments for this command.

Defaults

There are no default values.

Command Modes

MQC class-map configuration submode.

Command History

Release	Modification
12.4(15)XM	This command was introduced.

Examples

The following example illustrates the **match flow mip-bind** command:

```
Router(config-cmap)# match flow mip-bind
```

match flow pdp

To classify an HA flow, use the **match flow pdp** command in global class-map configuration mode.

match flow pdp

no match flow pdp

Syntax Description

There are no keywords or arguments for this command.

Defaults

There are no default values.

Command Modes

Global class-map configuration.

Command History

Release	Modification
12.4(15)XM	This command was introduced.

Examples

The following example illustrates the **match flow pdp** command:

```
Router(conf t)# class-map <class-name>
Router(config-cmap)#match flow ?
pdp PDP context of flow
Router(config-cmap)# match flow pdp
Router(config-cmap)# end
```

police rate mip-binding

To police the individual MN binding already identified to MQC, based on the specified rate, use the **police rate mip-binding** command specified in policy-map config mode specific to a configured class. Use the **no** form of the command to disable this feature.

police rate mip-binding [bc *bytes***] [peak-rate mip-binding [be** *bytes***]]**

no police rate mip-binding [bc *bytes***] [peak-rate mip-binding [be** *bytes***]]**

Syntax Description

bc *bytes*	Specifies the.
peak-rate mip-binding	Specifies the peak rate mip binding.
be *bytes*	Specifies the

Defaults

There are no default values.

Command Modes

Policy-map configuration submode.

Command History

Release	Modification
12.4(15)XM	This command was introduced.

Examples

The following example illustrates the **police rate mip-binding** command:

```
Router (config-pmap-c)# class-map class-mip
   match flow mip-binding
policy-map policy-mip-flow
class class-mip
   police rate mip-binding [bc bytes] [peak-rate mip-binding [be byes]] conform-action
action exceed-action action violate-action action
```

police rate pdp

To invoke police action on a binding flow, use the **police rate pdp** command in global policy-map configuration mode.

police rate pdp [**burst** *bytes*] [**peak-rate pdp** [**peak-burst** *bytes*]] **conform-action** *action* [**exceed-action** *action* [**violate-action** *action*]]

no police rate pdp [**burst** *bytes*] [**peak-rate pdp** [**peak-burst** *bytes*]] **conform-action** *action* [**exceed-action** *action* [**violate-action** *action*]]

Syntax Description

burst	Specifies the burst parameter.
peak-rate pdp	Specifies the peak rate pdp binding.
peak-burst	Specify **peak-burst** parameter for **peak-rate**
conform-action	Specifies action when rate is less than conform burst.
exceed-action	Specifies action taken when rate is within conform and conform + exceed burst
violate-action	Specifies action when rate is greater than conform + exceed burst

Defaults

There are no default values.

Command Modes

Policy-map configuration submode.

Command History

Release	Modification
12.4(15)XM	This command was introduced.

Usage Guidelines

The **peak-rate pdp** parameter ensures that policing is done based on a rate specified for each binding flow. The actual rate is specified using the **mobile ip** command described above.

The **peak-rate pdp** parameter has the following restrictions:

- You cannot remove one of the policies (either input or output) if both policies are configured.
- You cannot modify the existing service-policy for a realm without unconfiguring and then reconfiguring it.
- You cannot configure output-policy first and then input policy.

Examples

The following example illustrates the **police rate pdp** command:

```
Router(config)# policy-map <policyname>
Router(config)# class <class-name>
Router(config-pmap-c)# ?
   police           Police
Router(config-pmap-c)#police ?
      <8000-2000000000>  Bits per second
      cir                Committed information rate
```

```
      rate               Specify police rate
Router(config-pmap-c)#police rate ?
     pdp              APN PDP context
Router(config-pmap-c)#police rate pdp ?
      burst           Specify 'burst' parameter
      conform-action  action when rate is less than conform burst
      peak-burst      Specify 'peak-burst' parameter for 'peak-rate'
      peak-rate       Specify peak rate
      <cr>
Router(config-pmap-c)#police rate pdp burst 1000 peak-rate  ?
      pdp             APN PDP context
Router(config-pmap-c)#police rate pdp burst 1000 peak-rate pdp ?
      conform-action  action when rate is less than conform burst
      peak-burst      Specify 'peak-burst' parameter for 'peak-rate'
Router(config-pmap-c)#police rate pdp burst 1000 peak-rate pdp peak-burst 5000 ?
      conform-action  action when rate is less than conform burst
      <cr>
Router(config-pmap-c)#police rate pdp burst 1000 peak-rate pdp peak-burst 5000
conform-action <transmit> ?
      exceed-action  action when rate is within conform and conform + exceed burst
      <cr>
Router(config-pmap-c)#police rate pdp burst 1000 peak-rate pdp peak-burst 5000
conform-action <transmit> exceed-action <drop> ?
      violate-action  action when rate is greater than conform + exceed burst
      <cr>
```

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** global configuration command. 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
12.1T	This command was introduced.

Usage Guidelines

Using the **radius-server attribute 32 include-in-access-req** 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:

```
router (config)# 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 attribute 55 access-request include

To send RADIUS attribute 55 Event-Timestamp in Access-Request, use the **radius-server attribute 55 access-request include** global configuration command. To disable sending this attribute, use the **no** form of this command.

radius-server attribute 55 access-request include

no radius-server attribute 55 access-request include

Syntax Description

There are no keywords or arguments.

Defaults

There are no default values.

Command Modes

Global configuration.

Command History

Release	Modification
12.4(15)XM	This command was introduced.

Usage Guidelines

Examples

The following example illustrates how to configure the **radius-server attribute 55 access-request include** command:

```
router (config)# radius-server attribute 55 access-request include
```

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*} [**auth-port** *port-number*] [**acct-port** *port-number*] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*] [**alias** {*hostname* | *ip-address*}]

no radius-server host {*hostname* | *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*] [**alias** {*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.
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.
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.
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. Range is from 0 to 100 where “0” nullifies the retransmissions. 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.

Defaults

The **auth-port** port number defaults to 1645; the **acct-port** port number defaults to 1646.

Command Modes

Global configuration

Command History

Release	Modification
12.2(2)XC	This command was introduced.

Examples

The following example shows the **radius-server host** command:

```
Router# radius server host 20.1.1.1
```

radius-server vsa send accounting wimax

To configure the WiMAX VSAs included in RADIUS accounting messages generated by the HA, use the **radius-server vsa send accounting wimax** command in global configuration mode. Use the **no** form of the command to disable this feature.

radius-server vsa send accounting wimax

no radius-server vsa send accounting wimax

Syntax Description

There are no keywords or arguments for this command.

Defaults

There are no default values.

Command Modes

Global configuration

Command History

Release	Modification
12.4(15)XM	This command was introduced.

Usage Guidelines

When this command is enabled, the following following RADIUS attributes will be included in accounting messages generated by the HA.

- Acct-Terminate-Cause (49)
- Acct-Multi-Session-Id (50)
- Acct-Session-Time (46)
- Chargeable-User-Identity(89)
- Acct-Input-Gigawords (52)
- Acct-Output-Gigawords (53)
- HA-IP-MIP4 (26/2)
- GMT-Time-Zone-Offset (26/3)

Examples

The following example shows the **radius-server vsa send accounting wimax** command:

```
Router# radius-server vsa send accounting wimax
```

radius-server vsa send authentication wimax

To configure WiMAX VSAs included in RADIUS Access-Request messages, use the **radius-server vsa send authentication wimax** command in global configuration mode. Use the **no** form of the command to disable this feature.

radius-server vsa send authentication wimax

no radius-server vsa send authentication wimax

Syntax Description

There are no keywords or arguments for this command.

Defaults

There are no default values.

Command Modes

Global configuration

Command History

Release	Modification
12.4(15)XM	This command was introduced.

Usage Guidelines

When this command is enabled, the following following RADIUS attributes will be included in Access-Request messages generated by the HA.

- Acct-Interim-Interval (85)
- Message-Authenticator(80)
- Chargeable-User-Identity(89)
- WiMAX Capability (26/1)
- HA-IP-MIP4 (26/2)
- RRQ-HA-IP (26/18)
- MN-HA-MIP4-SPI (26/11)
- RRQ-MN-HA-SPI (26/20)

Examples

The following example shows the **radius-server vsa send authentication wimax** command:

```
Router# radius-server vsa send authentication wimax
```

redirect ip access-group

To specify that IP be the redirected profile-based configuration, use the **redirect ip access-group** command in hotline-rules sub-command configuration mode. Use the **no** form of the command to disable this feature.

redirect ip access-group { *acl-no* | *word* } {**in | out**} {**redirect** *ip-addr* [**port**]}

no redirect ip access-group { *acl-no* | *word* } {**in | out**} {**redirect** *ip-addr* [**port**]}

Syntax Description

acl-no	Specifies the ACL number. ACL numbers range from 100-199 & 2000-2699.
word	Specifies the nai realm in the format of *username@cisco.com*. Otherwise, the command gives an error message.
in	Specifies that redirects occur
out	Specifies that redirects
redirect *ip-addr*	Specifies the IP address of the redirected user.
port	Specifies the port number for the redirected user.

Defaults

There are no default values.

Command Modes

Global configuration

Command History

Release	Modification
12.4(15)XM	This command was introduced.

Usage Guidelines

The configured acl should be an extended acl. ACL numbers range from 100-199 & 2000-2699.

Examples

The following example illustrates the **redirect ip access-group** command:

```
redirect ip access-group 100 in redirect 20.20.20.20 1
```

router mobile

To enable Mobile IP on the router, use the router mobile global configuration command. 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 will remove all related configuration commands, both global and interface.

Examples

The following example enables Mobile IP:

```
Router# router mobile
```

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** | **qos police flowid** *id* | **police nai** *@example.com*]

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) Total number of bindings in the table.
vrf	(Optional) VRF of the user.
qos police flowid *id*	(Optional) Displays details such as police rate (PIR, and CIR values) in kbps, and the packets that have conformed, exceeded, or violated the rate.
police nai	(Optional) Displays when QoS policing is enabled and statistics for each individual binding.

Command Modes

Privileged 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)XM	The **qos police flowid** keyword was introduced, and .

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
Total VPDN Tunnel'ed 1
mip-lac-user1@ispxyz.com (Bindings 1):
    Home Addr 30.0.0.5
    Care-of Addr 7.0.0.1, Src Addr 7.0.0.1
```

```
    Lifetime granted 00:30:00 (1800), remaining 00:28:56
    Flags sBdmg-T-, Identification CA932143.10000
    Tunnel0 src 7.0.0.2 dest 7.0.0.1 reverse-allowed
    Routing Options - (B)Broadcast (T)Reverse-tunnel
    Service Options:
        VPDN Tunnel (setup-time 90 secs)
    Revocation negotiated - I-bit set
```

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
```

Here is an example of the **show ip mobile binding police nai** command:

```
Router#show ip mobile binding police nai <@example.com>
    Mobility Binding List:
    user1@cisco.com (Bindings 1):
    DOWNLINK POLICING STATISTICS

      police:
          rate 8000 , bc 1400 bytes
         peak-rate 8000, be 1700 bytes
        conformed 1 packets, 204 bytes; actions:
          transmit
        exceeded 0 packets, 0 bytes; actions:
          transmit
        violated 0 packets, 0 bytes; actions:
          drop
```

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.
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 vrf

To display all the bindings on the HA that are VRF-enabled, use the **show ip mobile binding vrf** EXEC command.

show ip mobile binding vrf [**summary**]

Syntax Description

summary	(Optional) Displays the total number of bindings that are VRF-enabled.

Command Modes

EXEC

Command History

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

Usage Guidelines

This command does not show those bindings that are in default routing table.

Examples

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

```
Router#show ip mobile binding vrf
Mobility Binding List:
    Total number of VRF bindings 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 00:03:02
    Flags sBdmg-T-, Identification C6DEF608.10000
    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: 11
    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
```

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 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
```

show ip mobile binding vrf realm

To display all bindings for the realm that are VRF-enabled, use the **show ip mobile binding vrf realm** EXEC command.

show ip mobile binding vrf realm *realm-name* [**summary**]

Syntax Description

summary	(Optional) Displays the total number of bindings for the realm that are VRF-enabled.

Command Modes

EXEC

Command History

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

Examples

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

```
Router#show ip mobile binding vrf realm @cisco.com
Mobility Binding List:
Total bindings for realm @cisco.com under VRF moip-vrf is 1
cisco-moip1@cisco.com (Bindings 1):
    Home Addr 5.5.5.5
    Care-of Addr 92.92.92.1, Src Addr 92.92.92.1
    Lifetime granted 00:25:00 (1500), remaining 00:11:05
    Flags sbdmg-T-, Identification C3BC05F8.10000
    Tunnel0 src 192.168.11.1 dest 92.92.92.1 reverse-allowed
    Routing Options - (T)Reverse-tunnel
    VRF moip-vrf (id=1)
```

show ip mobile globals

To display global information for Mobile Agents, use the **show ip mobile globals** EXEC command.

show ip mobile globals

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.3(7)XJ	Radius Disconnect and MIP Revocation statistics were added.

Usage Guidelines

This command shows which services are provided by the Home Agent and/or Foreign Agent. Note the deviation from RFC 2006; 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 when both Radius Disconnect and MIP Revocation are enabled on HA:

```
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 disabled
    NAT Traversal disabled
    HA Accounting enabled using method list: mylist
    NAT UDP Tunneling support enabled
    UDP Tunnel Keepalive 600
    Forced UDP Tunneling disabled
    Address 7.0.0.2    -------->>>>>> Redundant HA information
    Standby groups
    cisco
    Virtual networks
    40.0.0.0 /8

    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
Radius Disconnect Capability disabled
```

Table 10 describes the significant fields shown in the display.

Table 10 show ip mobile globals Field Descriptions

Field	Description
Home Agent	
Registration lifetime	Default lifetime 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	Broadcast enabled or disabled.
Reverse tunnel	Reverse tunnel enabled or disabled.
ICMP Unreachable	Send ICMP Unreachable enabled or disabled for virtual network.
Virtual networks	List virtual networks serviced by Home Agent. Displayed if defined.
Foreign Agent	
Care-of addresses advertised	List care-of addresses (interface is up or down). Displayed if defined.
Mobility Agent	
Number of interfaces providing service	See the **ip mobile interface** command for more information on advertising. Agent advertisements are sent when IRDP is enabled.
Encapsulation supported	IPIP and GRE.
Tunnel fast switching	Tunnel fast switching enabled or disabled.
Discovered tunnel MTU	Aged out after amount of time.

show ip mobile host

To display mobile station counters and information, use the **show ip mobile host** EXEC command.

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

EXEC

Command History

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

Examples

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

```
Router# show ip mobile host
Mobile Host List:

Total 5
mwts-mip-r20sit-haslb@ispxyz.com:
    Dynamic address from AAA pool mobilenodes
    Allowed lifetime 00:10:00 (600)
    Roam status -Registered-, Home link on virtual network 40.0.0.0 /8
    Bindings
         40.0.0.2
    Accepted 0, Last time -never-
    Overall service time 00:00:39
    Denied 0, Last time -never-
    Last code '-never- (0)'
    Total violations 0
    Acct-Session-Id: 43
    Sent on tunnel to MN: 0 packets, 0 bytes
    Received on reverse tunnel from MN: 0 packets, 0 bytes
    Input ACL: mipinacl
    Output ACL: mipoutacl
mwts-pmp-r20sit-base-user1@ispxyz.com:
    Dynamic address from local pool mobilenodes
    Allowed lifetime 00:08:20 (500)
    Roam status -Unregistered-, Home link on virtual network 40.0.0.0 /8
```

```
router#
```

Table 11 describes the significant fields shown in the display.

Table 11 show ip mobile host Field Descriptions

Field	Description
IP address	Home IP address of the mobile node.
Allowed lifetime	Allowed lifetime 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 (Code 0 + Code 1).
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 Home Agent last rebooted.
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 station	Number of packets and bytes tunneled to mobile node.
Reverse tunnel from mobile station	Number of packets and bytes reverse tunneled from mobile node.

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

mwtr-pmp-user1
Dynamic address from AAA server
Dynamic address from local pool mobilenodes
Static address authorization by AAA server
Static address authorization using local pool mobilenodes
Home link on virtual network 30.0.0.0 /8, Care-of ACL -none-
Security associations on AAA server, stored remotely

Allowed lifetime (INFINITE)
```

Table 12 describes the significant fields shown in the display.

Table 12 show ip mobile host group Field Descriptions

Field	Description
IP address	Mobile host IP address or grouping of addresses.
Home link	Interface or virtual network.
Care-of ACL	Care-of address access list.
Security association	Router or AAA server.
Allowed lifetime	Allowed lifetime for mobile host or group.

Related Commands

Command	Description
show ip mobile binding	Displays the mobility binding table.
clear ip mobile host-counters	Clears the mobile station-specific counters.

show ip mobile hotline

To display a list of hotline profiles or a particular hotline profile, use the **show ip mobile hot-line** EXEC command.

show ip mobile hotline {**profile** [*profile-id*] | **summary** | **users** [**nai** *id*] }

Syntax Description

profile	Displays information about a specific profile that is hotlined on the HA.
summary	Displays summary information for a specific profile or group of profiles.
users	Displays the MN specified by the **nai** *id.*
nai *id*	Displays the **nai** *id* of a specific user or users.

Defaults

There are no default values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(15)XM	This command was introduced.

Examples

The following example illustrates the **show ip mobile hotline** command:

```
show ip mobile hotline users ?
  nai  MN identified by NAI
  |    Output modifiers
  <cr>
```

The following is the sample output.

```
HA#show ip mobile hotline users nai mip1@cisco.com
blrmip1@cisco.com (Bindings 1):
  Rule Based HotLining (Rules 1)
    RuleType HTTPPRedir, Dynamic ACL Number 10
    Direction - in
    Redirect url - www.cisco.com

HA#show ip mobile hotline users
Hotline Binding List:
blrmip1@cisco.com (Bindings 1):
  Rule Based HotLining (Rules 1)
    RuleType HTTPPRedir, Dynamic ACL Number 10
    Direction - in
    Redirect url - www.cisco.com

blrmip2@cisco.com (Bindings 1):
  Rule Based HotLining (Rules 1)
    RuleType HTTPPRedir, Dynamic ACL Number 10
    Direction - in
    Redirect url - www.cisco.com
```

This command displays the list of hotline profiles or a particular hotline profile.

```
show ip mobile hotline profile ?
  WORD  Profile-Id
  |     Output modifiers
  <cr>
```

The following is sample output:

```
HA#Show ip mobile hotline profile cisco
Hotline Profile List:
 Profile: cisco (Rules 1)
    RuleType HTTPRedir, Extended ACL Number 100
    Direction - in
    Redirected Url - cisco.com

HA#show ip mobile hotline profile
Hotline Profile List:
Total 2
 Profile: cisco (Rules 1)
    RuleType HTTPRedir, Extended ACL Number 100
    Direction - in
    Redirected Url - cisco.com

 Profile: ht-prof1 (Rules 3)
    RuleType IPRedir, Extended ACL Name ht-acl1
    Direction - in
    Redirected IPAddr 16.1.1.102

    RuleType IPRedir, Extended ACL Number 100
    Direction - in
    Redirected IPAddr 1.1.1.1

    RuleType IPFilter, Extended ACL Name cisco
    Direction - out
    HA#
```

This command displays the current hotlining statictics.

```
show ip mobile hotline profile ?
|     Output modifiers
   <cr

HA#sh ip mob hot summary
HomeAgent Hotlining Summary:
    Number of Sessions Hotlined 2
    Number of Profile-Based Hotlined 0
    Number of Rule-Based Hotlined 2
HA#
```

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** EXEC command.

show ip mobile secure {**host** | **visitor** | **foreign-agent** | **home-agent** | **proxy-host** | **summary** | **rk**} {*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 Home Agent on the Foreign 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 the table.
rk	Displays the registration keys.
ip-address	IP address of non-nai mobile node. For mobile node with nai option, the host information is not displayed by ip-address option.
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** and **proxy-host** keywords were 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 home-agent

Security Associations (algorithm,mode,replay protection,key):
20.0.0.6
    SPI 300,  MD5, Prefix-suffix, Timestamp +/- 7,
    Key 00112233445566778899001122334455
```

Table 13 describes the significant fields shown in the display.

Table 13 show ip mobile secure Field Descriptions

Field	Description
IP address	IP address.
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.
Prefix-suffix	Authentication mode.
Timestamp	Replay protection method.
Key	The shared secret key for the security associations, in hexadecimal format.

The downloaded HA-RK key, SPI and lifetime can be displayed using the following command:

```
Router#show ip mobile secure home-agent ha-rk [ha-ip]
HomeAgent HA-RK List:
15.1.1.80:
    SPI 102, Lifetime 00:10:30 (630), Remaining 00:10:24
    Key 31323334353637383930313233334353637383930
```

The generated FA-HA-Keys can be displayed using the following command:

```
Router#show ip mobile secure foreign-agent [fa-ip]

e.g. Router#show ip mobile secure foreign-agent

Security Associations (algorithm,mode,replay protection,key):
14.1.1.28:
    SPI 102,  HMAC-MD5, Timestamp +/- 7, HA-IP 15.1.1.80
    Key b932c46406dcfe411f8bd147103ac53ca0c7fe65
```

The above downloaded HA-RK and generated FA-HA-keys are deleted if HA-RK lifetime is expired or a new HA-RK key is downloaded for the same HA-IP.

show ip mobile traffic

To display Home Agent protocol counters, and to incorporate cumulative counters for hot-lined sessions, use the **show ip mobile traffic** EXEC command.

show ip mobile traffic [**since**]

Syntax Description

since	Displays the cumulative counters for hot-lined sessions.

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.3(7)XJ	MIPv4 Registration Revocation message related statistics were added.
12.3(7)XJ1	New counters for Bind Delete Request and Ack messages were introduced.
12.4(15)XM	This command was enhanced to show hotlining counters.

Usage Guidelines

Counters can be reset to zero (0) 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

sh ip mob traffic
IP Mobility traffic:
Time since last cleared: 1d06h
Advertisements:
    Solicitations received 0
    Advertisements sent 0, response to solicitation 0
Home Agent Registrations:
    Register requests rcvd 2, denied 0, ignored 0, dropped 0, replied 2
    Register requests accepted 2, No simultaneous bindings 0
    Register requests rcvd initial 1, re-register 0, de-register 1
    Register requests accepted initial 1, re-register 0, de-register 1
    Register requests replied 1, de-register 1
    Register requests denied initial 0, re-register 0, de-register 0
    Register requests ignored initial 0, re-register 0, de-register 0
    Registration Request Errors:
      Unspecified 0, Unknown HA 0, NAI check failures 0
      Administrative prohibited 0, No resource 0
      Authentication failed MN 0, FA 0, active HA 0
      Bad identification 0, Bad request form 0
      Unavailable encap 0, reverse tunnel 0
      Reverse tunnel mandatory 0
      Unrecognized VendorID or CVSE-Type in CVSE sent by MN to HA 0
```

```
      Unrecognized VendorID or CVSE-Type in CVSE sent by FA to HA 0
    Binding Updates received 0, sent 2 total 2 fail 0
    Binding Update acks received 2 sent 0
    Binding info requests 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
    Binding Delete Req received 0, sent 0 total 0 fail 0
    Binding Delete acks received 0 sent 0
    Binding Sync Req received 0, sent 0 total 0 fail 0
    Binding Sync acks received 0 sent 0
    Gratuitous 0, Proxy 0 ARPs sent
    Route Optimization Binding Updates sent 0, acks received 0 neg acks received 0
    Registration Revocation msg sent 0 rcvd 0 ignored 0
    Registration Revocation acks sent 0 rcvd 0 ignored 0
    Total incoming registration requests using NAT detect 0

RADIUS DISCONNECT:
  Disconnect Request rcvd 0, accepted 0
  Disconnect Request Errors:
    Unsupported Attribute 0, Missing Attribute 0
    Invalid Request 0, NAS Id Mismatch 0
    Session Cxt Not Found 0, Administratively Prohibited 0


Change of Authorization:
  Request rcvd 0, accepted 0
  Request Errors:
    Unsupported Attribute 0, Missing Attribute 0
    Invalid Request 0, NAS Id Mismatch 0
    Session Cxt Not Found 0, Session Cxt Not Removable 0
    Unsupported Service 0

Dynamic DNS Update (IP Reachability):
  Number of DDNS Update Add request sent 2
  Number of DDNS Update Delete request sent 2

router#
```

The following example displays hotlining counters:

```
HA# show ip mobile traffic
IP Mobility traffic:
Advertisements:
    Solicitations received 0
    Advertisements sent 0, response to solicitation 0
Home Agent Registrations:
    Register requests rcvd 1351, denied 0, ignored 0, dropped 0, replied 1
    Register requests accepted 1351, No simultaneous bindings 0
    Register requests rcvd initial 149, re-register 1132, de-register 70
    Register requests accepted initial 149, re-register 113, de-register 7
    Register requests replied 1281, de-register 70
    Register requests denied initial 0, re-register 0, de-register 0
    Register requests ignored initial 0, re-register 0, de-register 0
    Registration Request Errors:
      Unspecified 0, Unknown HA 0, NAI check failures 0
      Administrative prohibited 0, No resource 0
      Authentication failed MN 0, FA 0, active HA 0
      Bad identification 0, Bad request form 0
      Unavailable encap 0, reverse tunnel 0
      Reverse tunnel mandatory 0
      Unrecognized VendorID or CVSE-Type in CVSE sent by MN to HA 0
      Unrecognized VendorID or CVSE-Type in CVSE sent by FA to HA 0
    Binding Updates received 14, sent 0 total 0 fail 1351
```

```
    Binding Update acks received 0 sent 14
    Binding info requests received 0, sent 1 total 2 fail 1
    Binding info reply received 1 drop 0, sent 0 total 0 fail 0
    Binding info reply acks received 0 drop 0, sent 1
    Binding Delete Req received 0, sent 0 total 0 fail 0
    Binding Delete acks received 0 sent 0
    Binding Sync Req received 0, sent 0 total 0 fail 0
    Binding Sync acks received 0 sent 0
    Gratuitous 0, Proxy 0 ARPs sent
    Route Optimization Binding Updates sent 0, acks received 0 neg acks received 0
    Registration Revocation msg sent 0 rcvd 0 ignored 0
    Registration Revocation acks sent 0 rcvd 0 ignored 0
    Total incoming registration requests using NAT detect 0

    Total VPDN Tunnel sessions attempted: 1 success: 1 fail: 0 pending: 0
                               PPP IDBS: 1 no resource: 0 deleted: 0


Change of Authorization:
  Request rcvd 0, accepted 0
  Request Errors:
    Unsupported Attribute 0, Missing Attribute 0
    Invalid Request 0, NAS 0
    Session Cxt Not Found 0, Session Cxt Not Removable 0
    Unsupported Service 0
Dynamic DNS Update (IP Reachability):
Number of DDNS Update Add request sent 0
  Number of DDNS Update Delete request sent 0
Home Agent Hotlining:
    Number of Hotline Sessions 6
    Number of Active-Session Hotlined 0
    Number of New-Session Hotlined 6
    Number of Active-Sessions Reconciled 0
    Number of New-Sessions Reconciled 0

HA#
```

Note "received" is the number of messages received, "sent" is the total number of messages sent, "Total" includes retransmissions, and "fail" is the number of messages that failed to be sent out.

Table 14 describes the significant fields shown in the display.

Table 14 show ip mobile traffic Field Descriptions

Field	Description
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 mobility agent in response to mobile node solicitations.
Home Agent	
Register requests	Total number of Registration Requests received by Home Agent.
Deregister requests	Total number of Registration Requests received by the Home Agent with a lifetime of zero (requests to deregister).

Table 14 show ip mobile traffic Field Descriptions (continued)

Field	Description
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 Home Agent (Code 0).
No simultaneous binding	Total number of Registration Requests accepted by Home Agent—simultaneous mobility bindings unsupported (Code 1).
Denied	Total number of Registration Requests denied by Home Agent.
Ignored	Total number of Registration Requests ignored by Home Agent.
Unspecified	Total number of Registration Requests denied by Home Agent—reason unspecified (Code 128).
Unknown HA	Total number of Registration Requests denied by Home Agent—unknown Home Agent address (Code 136).
Administrative prohibited	Total number of Registration Requests denied by Home Agent—administratively prohibited (Code 129).
No resource	Total number of Registration Requests denied by Home Agent—insufficient resources (Code 130).
Authentication failed MN	Total number of Registration Requests denied by Home Agent—mobile node failed authentication (Code 131).
Authentication failed FA	Total number of Registration Requests denied by Home Agent—Foreign Agent failed authentication (Code 132).
Bad identification	Total number of Registration Requests denied by Home Agent—identification mismatch (Code 133).
Bad request form	Total number of Registration Requests denied by Home Agent—poorly formed request (Code 134).
Unavailable encapsulation	Total number of Registration Requests denied by Home Agent—unavailable encapsulation (Code 139).
Unavailable reverse tunnel	Total number of Registration Requests denied by Home Agent—reverse tunnel unavailable (Code 137).
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.
Foreign Agent	
Request in	Total number of Registration Requests received by Foreign Agent.
Forwarded	Total number of Registration Requests relayed to Home Agent by Foreign Agent.
Denied	Total number of Registration Request denied by Foreign Agent.
Ignored	Total number of Registration Request ignored by Foreign Agent.
Unspecified	Total number of Registration Requests denied by Foreign Agent—reason unspecified (Code 64).
HA unreachable	Total number of Registration Requests denied by Foreign Agent—Home Agent unreachable (Codes 80-95).

Table 14 show ip mobile traffic Field Descriptions (continued)

Field	Description
Administrative prohibited	Total number of Registration Requests denied by Foreign Agent—administratively prohibited (Code 65)
No resource	Total number of Registration Requests denied by Home Agent— insufficient resources (Code 66).
Bad lifetime	Total number of Registration Requests denied by Foreign Agent— requested lifetime too long (Code 69).
Bad request form	Total number of Registration Requests denied by Home Agent—poorly formed request (Code 70).
Unavailable encapsulation	Total number of Registration Requests denied by Home Agent— unavailable encapsulation (Code 72).
Unavailable compression	Total number of Registration Requests denied by Foreign Agent— requested Van Jacobson header compression unavailable (Code 73).
Unavailable reverse tunnel	Total number of Registration Requests denied by Home Agent—reverse tunnel unavailable (Code 74).
Replies in	Total number of well-formed Registration Replies received by Foreign Agent.
Forwarded	Total number of valid Registration Replies relayed to the mobile node by Foreign Agent.
Bad	Total number of Registration Replies denied by Foreign Agent—poorly formed reply (Code 71).
Ignored	Total number of Registration Replies ignored by Foreign Agent.
Authentication failed MN	Total number of Registration Requests denied by Home Agent—mobile node failed authentication (Code 67).
Authentication failed HA	Total number of Registration Replies denied by Foreign Agent—Home Agent failed authentication (Code 68).

show ip mobile tunnel

To display information about the mobile IP tunnel, use the **show ip mobile tunnel** EXEC command.

show ip mobile tunnel *tunnel* [**summary**]

Syntax Description

tunnel	Displays the tunnel interface.
summary	(Optional) Displays a summary of the tunnels.

Command Modes

EXEC

Command History

Release	Modification
12.3(7)XJ	This command was introduced.
12.x(xx)x	The **summary** keyword was added.

Usage Guidelines

Note The source IP address of the tunnel is the IP address configured corresponding to the VRF. The VRF applied on the tunnel idb is also displayed

Examples

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

```
Router#show ip mobile tunnel
Mobile Tunnels:

Total mobile ip tunnels 1
Tunnel0:
    src 20.20.202.102, dest 20.20.210.10
    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 GigabitEthernet0/0.202
    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
    Template configuration:
        ip access-group 150 in

Router#
```

ACLs Applied to a Mobility Binding

```
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
```

show ip mobile violation

To display information about security violations, use the **show ip mobile violation** EXEC command.

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.

Usage Guidelines

The most recent violation is saved for all the mobile nodes. A circular log holds up to 50 unknown requesters, violators without security association. 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 15 describes significant fields shown in the display.

Table 15 show ip mobile violation Field Descriptions

Field	Description
20.0.0.1	IP address of the violator.
Violations	Total number of security violations for this peer.
Last time	Time of the most recent security violation for this peer.

Table 15 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	Reason for the most recent security violation for this peer. Possible reasons are: • No mobility security association • Bad authenticator • Bad identifier • Bad SPI • Missing security extension • Other

show ip route vrf

To check and display the routing table information corresponding to a VRF, use the **show ip route vrf** EXEC command.

show ip route vrf *vrf-name*

Syntax Description

vrf-name	The name of the specific VRF.

Command Modes

EXEC

Command History

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

Examples

The following is sample output from the **show ip route vrf** command:

```
Router#show ip route vrf moip-vrf

Routing Table: moip-vrf
Codes: C - connected, S - static, 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
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     4.0.0.0/32 is subnetted, 1 subnets
M       4.4.4.100 [3/1] via 92.92.92.1, 00:00:45, Tunnel0
C    192.168.10.0/24 is directly connected, Tunnel0
```

show policy-map apn realm

To display aggregate policing statistics for flows across the APN interface, use the **show policy-map apn** command in Privileged EXEC mode. Use the **no** form of the command to disable the feature.

show policy-map apn realm *example.com*

no show policy-map apn realm *example.com*

Syntax Description

example.com	The name of the mobile realm .

Defaults

There are no default values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(15)XM	This command was introduced.

Examples

The following example illustrates the **show policy-map apn realm** command:

```
Router#show policy-map apn realm @cisco.com
 Realm @cisco.com

  Service-policy input: perbindingpolice

    Class-map: class-mip (match-all)
      0 packets, 0 bytes
      Match: flow pdp
      police:
          rate pdp
         peak-rate pdp, be 1000 bytes
        conformed 0 packets, 0 bytes; actions: transmit
        exceeded 0 packets, 0 bytes; actions: drop
        violated 0 packets, 0 bytes; actions: drop

    Class-map: class-default (match-any)
      0 packets, 0 bytes
      Match: any
```

show vpdn

To display

snmp-server enable traps ipmobile

To configure 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
12.1(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.

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
```

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.

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.

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 virtual server configuration command. To remove the attributes, use the no form of this command.

virtual *ip-address* **{tcp | udp}** *port-number* **[service** *service-name***]**

no virtual

Syntax Description

ip-address	IP address for this virtual server instance, used by clients to connect to the server farm.
tcp	Performs load balancing for only TCP connections.
udp	Performs load balancing for only UDP connections.
port-number	(Optional) 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-number argument are as follows: Domain Name System: **dns 53** File Transfer Protocol: **ftp 21** HTTP over Secure Socket Layer: **https 443** 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** 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).
service	(Optional) Couple connections associated with a given service, such as HTTP or Telnet, so all related connections from the same client use the same real server.
service-name	Optional) Type of connection coupling. Currently, the only choice is **ftp**. Couple FTP data connections with the control session that created them.

Defaults

No default behavior or values.

Command Modes

SLB virtual server configuration

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.

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 the IOS SLB feature. 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**.

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.

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.

```
ip slb vserver PUBLIC_HTTP
virtual 10.0.0.1 tcp www
```

The following example illustrates how to enable the Mobile IP SLB feature. The *ip address* is the virtual Home Agent address to which registration requests from PDSN/FA will be sent. This command is configured on the SLB Supervisor.

```
Router(config)# ip slb vserver <name>
Router(config-slb-vserver)# virtual ip address udp 434 service ip mobile
```

Related Commands

Command	Description
ip slb vserver	Identifies a virtual server.
show ip slb vservers	Displays information about the virtual servers.