Cisco IOS Mobile Wireless Home Agent Command Reference

Release 12.4

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Text Part Number: 78-17458-01

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

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

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

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

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

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0601R)

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

Cisco IOS Mobile Wireless Home Agent Command Reference
© 2006 Cisco Systems, Inc. All rights reserved.

Introduction

This book lists new and revised commands pertaining to the Home Agent software. All other commands used with this feature are documented in the Cisco IOS Release 12.4 command reference publications.

Commands

This book documents all of the Cisco IOS software commands in Cisco IOS Release 12.4 for the Home Agent, in alphabetical order.

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.

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*}

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.

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.

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.

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.

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

10.0.0.1:
    Allowed lifetime 10:00:00 (36000/default)
    Roaming status -Unregistered-, Home link on virtual network 10.0.0.0/8
    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

10.0.0.1:
    Allowed lifetime 10:00:00 (36000/default)
    Roaming status -Unregistered-, Home link on virtual network 10.0.0.0/8
    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.

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 EXEC command.

clear ip mobile traffic

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

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

Usage Guidelines

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

This command clears all Mobile IP counters. The undo keyword restores the counters (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.

Defaults

There are no default values for this command.

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 new map 4 ipsec-manual
```

debug ip mobile advertise

To display advertisement information, use the **debug ip mobile advertise** EXEC command .

debug ip mobile advertise

no debug ip mobile advertise

Syntax Description

This command has no arguments or keywords.

Defaults

No default values.

Command Modes

EXEC mode

Command History

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

Examples

The following is sample output from the **debug ip mobile advertise** command. Table 1 describes significant fields shown in the display.

```
Router# 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: 14.0.0.31
Prefix Length ext: len=1 (8 )
```

Table 1 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.

debug ip mobile host

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

debug ip mobile host *acl*

no debug ip mobile host

Syntax Description

acl	(Optional) Access list.

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 10.0.0.6 on interface Ethernet1 using COA
14.0.0.31 HA 15.0.0.5 lifetime 30000 options sbdmgvT
MobileIP: Authenticated FA 15.0.0.31 using SPI 110 (MN 20.0.0.6)
MobileIP: Authenticated MN 11.0.0.6 using SPI 300

MobileIP: HA accepts registration from MN 11.0.0.6
MobileIP: Mobility binding for MN 11.0.0.6 updated
MobileIP: Roam timer started for MN 11.0.0.6, lifetime 30000
MobileIP: MH auth ext added (SPI 300) in reply to MN 11.0.0.6
MobileIP: HF auth ext added (SPI 220) in reply to MN 11.0.0.6

MobileIP: HA sent reply to MN 11.0.0.6
```

debug ip mobile redundancy

Use the **debug ip mobile host** 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 14.0.0.20 - sent
BindUpd to HA 11.0.0.3 HAA 11.0.0.4
00:19:21: MobileIP: HA standby maint started - cnt 1
00:19:21: MobileIP: MN 14.0.0.20 - HA rcv BindUpdAck accept from 11.0.0.3 HAA 11.0.0.4
00:19:22: MobileIP: HA standby maint started - cnt 1
```

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-agen**t *address*] [**broadcast**] [**care-of-access** *acl*] [**lifetime** *number*] [**replay** *seconds*] [**reverse-tunnel private-address | off**] [**roam-access** *acl*] [**strip-nai-realm**] [**suppress-unreachable**] [**local-timezone**] [**unknown** [**accept | deny**]] [**send-mn-address**]

no ip mobile home-agent [**broadcast**] [**care-of-access** *acl*] [**lifetime** *number*] [**replay** *seconds*] [**reverse-tunnel private address**] [**roam-access** *acl*] [**strip-nai-realm**] [**suppress-unreachable**] [**local-timezone**] [**unknown** [**accept | deny**]] [**send-mn-address**]

Syntax Description

home-agent *address*	(Optional) IP address of the Home Agent.
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.
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.
replay *seconds*	(Optional) Sets the replay protection time-stamp value. Registration received within this time is valid.
reverse-tunnel	(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.
private-address	Private Mobile IP addresses used for reverse tunneling.
off	(Optional) Disables reverse tunnel mode.
roam-access *acl*	(Optional) Controls which mobile nodes are permitted or denied to roam. By default, all specified mobile nodes can roam.
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 [**accept** | **deny**]	When **unknown 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 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.

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 2)

and sends a reply. (Replay codes are listed in Table 3.) A security violation is logged when foreign agent authentication, MH authentication, or Identification verification fails. (The violation reasons are listed in Table 4.)

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 2 describes how the home agent treats registrations with various bits set when authentication and identification are passed.

Table 2 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 3 lists the home agent registration reply codes.

Table 3 Home Agent Registration Reply Codes

Code	Reason
0	Accept.
1	Accept, no simultaneous bindings.
128	Reason unspecified.

Table 3 Home Agent Registration Reply Codes (continued)

Code	Reason
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 4 lists security violation codes.

Table 4 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 broadcast lifetime 7200
```

```
Router (config)#ip mobile home-agent reverse-tunnel ?
  off              Disable reverse tunnel mode
  private-address  Reverse Tunneling Mandatory for Private Mobile IP addresses
```

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 *list*

Syntax Description

list	Specifies the accounting method used to generate accouting records. The accounting method identified by *list* is configured using the **aaa accounting network** command.

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 list
```

ip mobile home-agent reject-static-addr

To configure the Home Agent (HA) to reject Registration Requests from Mobile Nodes (MNs) under certain conditions, use the **ip mobile home-agent reject-static-addr** command in global configuration mode.

ip mobile home-agent reject-static-addr

Syntax Description

This command has not arguments or keywords

Command Modes

Global configuration.

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 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 Registration Request 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 redundancy

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

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

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

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.

Defaults

No global home agent addresses are specified.

Command Modes

Global configuration command.

Command History

Release	Modification
12.0(2)T	This command was introduced.

Usage Guidelines

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

Examples

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

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

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 in global configuration mode.

ip mobile home-agent resync-sa *time*

Syntax Description

time	Specifies the time that the HA will use to initiate a resynchronization.

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 the time specified, and the MN fails authentication, then the HA will not requery the AAA server for another Security Association (SA).

If the MN reregisters with the HA, and the time between registrations is greater than the time specified, 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 host

To configure the mobile host or mobile node group, use the **ip mobile host** global configuration command. For the Packet Data Serving Node (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* | **dhcp-proxy-client** [**dhcp-server** *addr*]}} {**interface** *name* | **virtual-network** *network-address mask*}} [**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* | **dhcp-proxy-client** [**dhcp-server** *addr*]}} {**interface** *name* | **virtual-network** *network-address mask*}} [**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.
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.
aaa	(Optional) Retrieves security associations from a AAA (TACACS+ or RADIUS) server.
load-sa	(Optional) Stores security associations in memory after retrieval.
permanent	(Optional) Retrieves security associations in memory.
authorized-pool *pool*	Verifies the IP address assigned to the mobile if it is within the pool specified by *pname*.

skip-aaa-reauthentication	(Optional) 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.

Usage Guidelines

This command configures the mobile host or mobile node group (ranging from *lower* address to *upper* address) to be supported by the home agent. These mobile nodes belong to the network on an interface or a virtual network (via the **ip mobile virtual-network** command). The security association for each mobile host must be configured using the **ip mobile secure** command or downloaded from 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 5 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 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 5.

Table 5 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).
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.

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 11.0.0.1 20.0.0.3 virtual-network 11.0.0.0 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 12.0.0.0
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 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** [*seconds*] **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** *spi-out* | **spi** *spi*} **key hex** *string* [**replay timestamp** [*seconds*] **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.
seconds	(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

Global 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 crypto map local route
```

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** *address***]**

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

Syntax Description

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

Defaults

No home agent addresses are specified.

Command Modes

Global configuration.

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.0(2)T	The address keyword 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 11.0.0.1 255.0.0.0

int e0
 ip addr 11.0.0.1 255.0.0.0
 standby ip 1.0.0.10
 standby name SanJoseHA

int lo0
 ip addr 11.0.0.1 255.255.255.255
ip mobile home-agent
 ip mobile virtual-network 11.0.0.0 255.255.0.0 20.0.0.1
 ip mobile home-agent standby localHA virtual-network
 ip mobile secure home-agent 12.0.0.2 spi 100 hex 00112233445566778899001122334455
```

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 resent to a server, if that server is not responding or responding slowly. This setting overrides the global setting of the **radius-server retransmit** command.
retries	(Optional) Specifies the retransmit value. Enter a value in the range 1 to 100. If no retransmit value is specified, the global value is used.
key	(Optional) Specifies the authentication and encryption key used between the router and the RADIUS daemon running on this RADIUS server. This key overrides the global setting of the **radius-server key** command. If no key string is specified, the global value is used. The key is a text string that must match the encryption key used on the RADIUS server. Always configure the key as the last item in the **radius-server host** command syntax. This is because the leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in the key, do not enclose the key in quotation marks unless the quotation marks themselves are part of the key.
string	(Optional) Specifies the authentication and encryption key for all RADIUS communications between the router and the RADIUS server. This key must match the encryption used on the RADIUS daemon. All leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in your key, do not enclose the key in quotation marks unless the quotation marks themselves are part of the key.
alias	(Optional) Allows up to eight aliases per line for any given RADIUS server.

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
```

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**]

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.

Command Modes

EXEC

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.0(2)T	The following keyword and argument were added: • **home-agent** • *address*
12.1(2)T	The **summary** keyword was added.
12.2(2)XC	The **nai** keyword was added.

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
20.0.0.1:
    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
```

Table 6 describes the significant fields shown in the display.

Table 6 show ip mobile binding Field Descriptions

Field	Description
Total	Total number of mobility bindings.
IP address	Home IP address of the mobile node.
Care-of Addr	Care-of address of the mobile node.
Src Addr	IP source address of the Registration Request as received by the home agent. Will be either the collocated care-of address of a mobile node or an address of the foreign agent.
Lifetime granted	The lifetime granted to the mobile node for this registration. Number of seconds in parentheses.
Lifetime remaining	The time remaining until the registration is expired. It has the same initial value as lifetime granted, and is counted down by the home agent.
Flags	Registration flags sent by mobile node. Uppercase characters denote bit set.
Identification	Identification used in that binding by the mobile node. This field has two purposes: unique identifier for each request, and replay protection.
Tunnel	The tunnel used by the mobile node is characterized by the source and destination addresses, and reverse-allowed or reverse-off for reverse tunnel. The default is IPIP encapsulation, otherwise GRE will be displayed in the Routing Options field.
Routing Options	Routing options list all home agent-accepted services. For example, the V bit may have been requested by the mobile node (shown in the Flags field), but the home agent will not provide such service. Possible options are B (broadcast), D (direct-to-mobile node), G (GRE), and T (reverse-tunnel).

show ip mobile globals

To display global information for mobile agents, use the **show ip mobile globals** 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.

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:

```
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
    Virtual networks
        20.0.0.0/8

Foreign Agent is not enabled, no care-of address

0 interfaces providing service
Encapsulations supported: IPIP and GRE
Tunnel fast switching enabled
Discovered tunnel MTU aged out after 1:00:00
```

Table 7 describes the significant fields shown in the display.

Table 7 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** [**nai** *string*] | **summary**]

Syntax Description

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

Command Modes

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

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
```

Table 8 describes the significant fields shown in the display.

Table 8 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

20.0.0.1 - 20.0.0.20:
    Home link on virtual network 20.0.0.0 /8, Care-of ACL -none-
    Security associations on router, Allowed lifetime 10:00:00 (36000/default)
```

Table 9 describes the significant fields shown in the display.

Table 9 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 secure

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

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

Syntax Description

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

Command Modes

EXEC

Command History

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

Usage Guidelines

Multiple security associations can exist for each entity.

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

Examples

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

```
Router# show ip mobile secure

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

Table 10 describes the significant fields shown in the display.

Table 10 show ip mobile secure Field Descriptions

Field	Description
10.0.0.6	IP address. The NAI is displayed if configured.
In/Out SPI	The SPI is the 4-byte opaque index within the mobility security association that selects the specific security parameters to be used to authenticate the peer. Allows either “SPI” or “In/Out SPI.” The latter specifies an inbound and outbound SPI pair. If an inbound SPI is received, then outbound SPI will be used when a response is sent.
MD5	Message Digest 5 authentication algorithm. HMAC-MD5 id displayed if configured.
Prefix-suffix	Authentication mode.
Timestamp	Replay protection method.
Key	The shared secret key for the security associations, in hexadecimal format.

show ip mobile traffic

To display Home Agent protocol counters, use the **show ip mobile traffic** EXEC command.

show ip mobile traffic

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

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

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

IP Mobility traffic:
Advertisements:
    Solicitations received 0
    Advertisements sent 0, response to solicitation 0
Home Agent Registrations:
    Register requests rcvd 7242, denied 2, ignored 0, dropped 0, replied 7242
    Register requests accepted 7240, No simultaneous bindings 0
    Register requests rcvd initial 7241, re-register 0, de-register 1
    Register requests accepted initial 7239, re-register 0, de-register 1
    Register requests replied 7241, de-register 1
    Register requests denied initial 2, 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 2, 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 0 total 0 fail 0
    Binding Update acks received 0 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
    Gratuitous 0, Proxy 0 ARPs sent
    Route Optimization Binding Updates sent 0, acks received 0 neg acks received 0
```

Table 11 describes the significant fields shown in the display.

Table 11 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).
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).

Table 11 show ip mobile traffic Field Descriptions (continued)

Field	Description
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).
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 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 12 describes significant fields shown in the display.

Table 12 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.
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

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
```

Related Commands

Command	Description
snmp-server host	Specifies which host or hosts receive SNMP notifications.