Chapter 15

Configuring the Mobile IP Home Agent

This chapter describes how to configure the Mobile IP home agent on E-series routers.

NOTE: Currently, JUNOSe software does not support configuration of the Mobile IP foreign agent.

Mobile IP Overview

Mobile IP is a tunneling-based solution that enhances the utility of E-series routers at the edge of the network between fixed wire and wireless network domains. This tunneling-based solution enables a router on a user's home subnet to intercept and forward IP packets to users who roam beyond traditional network boundaries. Mobile IP is useful in environments where mobility is desired and the traditional land line dial-in model does not provide an adequate solution, and in environments where a wireless technology is used.

Traditionally, IP addresses are associated with a fixed network location. To achieve mobility, the mobile node assumes a secondary IP address that matches the new network and redirects the traffic bound to the primary or home address to the mobile node's new network. In the Mobile IP architecture, the two agents that accomplish this task are the home agent and the foreign agent.

When a mobile node roams into a new network, it negotiates with the foreign agent to get a secondary IP address, which is referred to as the care-of address (CoA). The mobile node registers this CoA with the home agent. The home agent then establishes a tunnel to the CoA if the tunnel is not established earlier.

NOTE: You need to establish only one tunnel between the home agent and the CoA. Demultiplexing of the traffic is done through IP address inspection.

Packets sent to the home address of the mobile node are redirected by the home agent through the tunnel to the CoA at the foreign agent. The foreign agent routes the packets to the mobile node's home address. If the mobile node's home address is a private address or if the foreign agent implements ingress filtering, a reverse tunnel from the CoA to the home agent is required.

You can use the Mobile IP home agent feature to configure the home agent within a virtual router. The home agent handles the following tasks:

- Agent discovery
- Registration
- Routing and forwarding

Mobile IP Agent Discovery

Mobile nodes use the agent discovery process to identify whether they are on their home network or have roamed into a different network (referred to as a foreign network). Both the foreign agent and the home agent periodically multicast their agent advertisements. You can also request an agent advertisement from the mobile node through Internet Control Message Protocol (ICMP) router solicitations.

Mobile IP Registration

The home agent receives the registration requests on UDP port 434. The registration request contains the IP router ID as the home agent IP address. The home agent can support static home address allocation and dynamic home address allocation.

Home Address Assignment

The mobile node's home address can either be preconfigured, or dynamically allocated by the Mobile IP home agent. If a nonzero home address is preconfigured, the home agent processes the registration request using the home address. If the home address is dynamically allocated, the mobile node submits a nonzero home address and requests the home agent to assign an IP address. The mobile node then uses the address provided by the home agent for subsequent registration requests, until the mobile node is rebooted or the registration expires.

Home address allocation is done by one of the existing AAA back-end address mechanisms, such as:

- By RADIUS
- From an address pool returned by RADIUS
- From a local pool
- By the DHCP server

Authentication

The home agent authenticates the requests based on RFC 3344—IP Mobility Support for IPv4 (August 2002). The mobile home authentication is verified and the authentication algorithm and key are retrieved by checking the security association indexed by the security parameter index (SPI) value. This verification results in a 128-bit key and the authentication algorithm with which to compute an MD-5 message digest over the registration request. The Mobile IP home agent supports both HMAC-MD5 and keyed-MD5 authentication algorithms. When the result of this computation matches the 128-bit authenticator, the mobile-home extension is authenticated.

If a security association is configured for the foreign agent, the foreign-home authentication extension is verified; otherwise, authentication success is based only on the mobile-home authenticator.

The home agent checks the identification (ID) field used for matching registration requests with response and protection against replay attacks. The home agent uses timestamp-based replay protection and the ID field represents a 64-bit Network Time Protocol (NTP)-formatted time value. By default, the timestamp must be within 7 seconds of the home agent configured time value.

AAA

You can store the security associations and configuration information remotely on a RADIUS server. You can use the **ip mobile secure host** command and the **ip mobile secure foreign-agent** command to configure the security association (MD-5 key) for a specified user, or for a group of users (also known as a domain) for the home agent. The home agent can configure the security association (MD-5 key) for a specified user or a group of users (domain).

Authentication is accomplished either by generating an authentication, authorization, and accounting (AAA) access-request or querying the locally configured security parameters, depending on whether or not you use the **aaa** keyword when you issue the **ip mobile host** command to configure the mobile node. For AAA authentication, you must include the **aaa** keyword; for local authentication, do not include the **aaa** keyword. If AAA authentication is enabled, AAA queries the security information from the RADIUS server.

When both the network access identifier (NAI) and IP address of the mobile node are present in the registration request, then the authentication request from Mobile IP to AAA has the NAI as the user name and the IP address as the hint IP address. If only the NAI is present in the registration request, then the NAI address is used as the user name with no hint IP address in the authentication request. If only the IP address (home address) is present in the registration request, then it is used as both the user name and the hint IP address in the authentication request. If both the NAI address and the IP address are missing from the registration request, then the registration request is rejected.

If the optional **aaa** keyword is present in the **ip mobile host** command, then the authentication parameters are obtained by querying AAA. The authentication algorithm and security key are retrieved by AAA based on its configuration, depending on the SPI provided in the registration request. If the **aaa** keyword is absent, then the home agent uses authentication parameters configured locally on the router to authenticate the registration request. In both cases, if security parameters are not retrieved, then the request for mobility service is rejected, a security violation error is logged, and no registration reply is generated.

When you configure the mobile host to use RADIUS authentication for home agent users by including the **aaa** keyword in the **ip mobile host** command, the Mobile IP home agent application generates a RADIUS access-request message. The RADIUS server then uses Juniper Networks vendor-specific attributes (VSAs) to provide the appropriate authentication algorithm and secure key for the authentication request.

For information about the specific Juniper Networks VSAs used for Mobile IP RADIUS-based authentication, see *JUNOSe Broadband Access Configuration Guide, Chapter 3, Configuring RADIUS Attributes* and *JUNOSe Broadband Access Configuration Guide, Chapter 6, RADIUS Attribute Descriptions*.

Subscriber Management

The Mobile IP home agent interoperates with the subscriber management application on E-series routers. The subscriber management application enables customers to dynamically provision new IP subscribers and quickly create new value-added services.

You can set up your subscriber management environment to create dynamic IP subscriber interfaces to provision subscribers and provide differentiated service delivery. In this configuration, the service parameters for an IP subscriber are bound to a dynamic IP subscriber interface.

During the registration process when the Mobile IP home agent has authenticated the subscriber with AAA, the home agent locates or creates the appropriate IP tunnel to carry the data traffic to the foreign agent. When Mobile IP obtains all of the parameters required for interface creation, including the tunnel ID and the authentication context, it directs the subscriber management application to create the dynamic IP subscriber interface.

During the re-registration process when there is a handoff from an initial Mobile IP foreign agent to a new Mobile IP foreign agent, the home agent authenticates the subscriber with AAA and locates or creates the appropriate IP tunnel to carry the data traffic to the new foreign agent. When Mobile IP obtains all of the parameters required for interface creation, it directs the subscriber management application to move the dynamic IP subscriber interface from the initial tunnel for the previous foreign agent to the new tunnel that points to the new foreign agent. If this was the last subscriber on the tunnel for the previous foreign agent, then the home agent directs the IP tunneling application to tear down the initial tunnel.

For more information about subscriber management, see *JUNOSe Broadband Access Configuration Guide, Chapter 22, Configuring Subscriber Management*. For more information about dynamic IP subscriber interfaces, see *JUNOSe Broadband Access Configuration Guide, Chapter 24, Configuring Subscriber Interfaces*.

Mobile IP Routing and Forwarding

The home agent supports both generic routing encapsulation (GRE) and Distance Vector Multicast Routing Protocol (DVMRP, also known as IP-in-IP) tunnel encapsulation for forward and reverse tunneling. When packets destined for the mobile node reach a home agent, the home agent encapsulates the packets and tunnels them to the CoA. Packets that exceed the maximum transmission unit (MTU) value of the tunnel are dropped and an ICMP error message is sent to the source IP address. Packets without an access route are returned to the source with an ICMP destination unreachable error message. For reverse tunnels, packets are de-tunneled and forwarded towards the next hop to the destination address.

For more information about configuring GRE and DVMRP dynamic IP tunnels, see *Chapter 11, Configuring Dynamic IP Tunnels*.

Mobile IP Platform Considerations

For information about modules that support the Mobile IP home agent on ERX-7xx models, ERX-14xx models, and the ERX-310 router:

- See *ERX Module Guide, Table 1, Module Combinations* for detailed module specifications.
- See *ERX Module Guide, Appendix A, Module Protocol Support* for information about the modules that support the Mobile IP home agent.

For information about modules that support the Mobile IP home agent on E120 routers and E320 routers:

- See *E120 and E320 Module Guide, Table 1, Modules and IOAs* for detailed module specifications.
- See *E120 and E320 Module Guide, Appendix A, IOA Protocol Support* for information about the modules that support the Mobile IP home agent.

Mobile IP References

For more information about Mobile IP, consult the following resources:

- RFC 2006—The Definitions of Managed Objects for IP Mobility Support using SMIv2 (October 1996)
- RFC 2486—The Network Access Identifier (January 1999)
- RFC 2794—Mobile IP Network Access Identifier Extension for IPv4 (March 2000)
- RFC 2865—Remote Authentication Dial In User Service (RADIUS) (June 2000)
- RFC 3024—Reverse Tunneling for Mobile IP, revised (January 2001)
- RFC 3344—IP Mobility Support for IPv4 (August 2002)

Before You Configure the Mobile IP Home Agent

Before you can configure the Mobile IP home agent on a virtual router, perform the following tasks:

1. Create a virtual router to enable the Mobile IP license.
2. (Optional) Configure the access list for filtering foreign agents.
3. Configure an IP interface, which is used as the care-of address.
4. Configure the router ID of the virtual router, which becomes the home agent IP address.
5. (Optional) Configure the B-RAS license.
6. (Optional) Configure a RADIUS authentication server on the router.
7. (Optional) Configure a RADIUS accounting server on the router.
8. Configure a loopback interface to be used as the primary interface for a tunnel.
9. Configure an interface profile for mobile host associations.
10. Configure a destination profile for dynamic GRE or DVMRP tunnels, as described in *Chapter 11, Configuring Dynamic IP Tunnels*.

The following example illustrates this procedure:

```
! Create a virtual router.
host1(config)#virtual-router test
! Configure an access list.
host1:test(config)#access-list test deny ip host 100.1.1.3 any log
! Configure an IP interface.
host1:test(config)#interface loopback 0
host1:test(config-if)#ip address 10.10.10.1 255.255.255.255
! Configure the IP router ID.
```

```
host1:test(config)#ip router-id 10.10.10.1
! Configure the B-RAS license.
host1:test(config)#license b-ras demo
! Configure an authentication server.
host1:test(config)#radius authentication server 10.209.13.234
host1:test(config-radius)#key secret
host1:test(config-radius)#udp-port 1812
host1:test(config-radius)#radius update-source-addr 10.209.12.2
! Configure an accounting server.
host1:test(config-radius)#radius accounting server 10.209.13.234
host1:test(config-radius)#key secret
host1:test(config-radius)#udp-port 1813
! Create the primary interface for the tunnel.
host1:test(config)#interface loopback 1
! Configure a profile for mobile host associations.
host1:test(config)#profile virDefault
```

For information about configuring virtual routers and access lists, see the *JUNOSe System Basics Configuration Guide*. For information about configuring IP interfaces, see the *JUNOSe IP, IPv6, and IGP Configuration Guide*.

For information about configuring B-RAS licenses, RADIUS authentication servers, and RADIUS accounting servers, see the *JUNOSe Broadband Access Configuration Guide*.

Configuring the Mobile IP Home Agent

To configure the Mobile IP home agent on a virtual router:

1. Configure a license for the Mobile IP home agent.
2. Configure the Mobile IP home agent settings.
3. Configure one or more mobile hosts.
4. Configure the Mobile IP security associations for mobile hosts.
5. Configure the Mobile IP security associations for foreign agents.
6. Assign an interface profile to be referenced by the Mobile IP home agent.
7. (Optional) Verify the Mobile IP configuration. See *Monitoring the Mobile IP Home Agent* on page 365.

The following example illustrates how you can configure a Mobile IP home agent on a virtual router named test:

```
! Configure the Mobile IP home agent license.
host1:test(config)#license mobile-ip home-agent demo
! Configure the Mobile IP home agent settings.
host1:test(config)#ip mobile home-agent care-of-access acl lifetime 2000 replay 255
reverse-tunnel-off
```

```
! Configure mobile hosts and their security associations.
host1:test(config)#ip mobile host 200.1.1.1 lifetime 200
host1:test(config)#ip mobile secure host 200.1.1.1 spi 0x398 key ascii w4ex
algorithm keyed-md5 replay timestamp within 225
! Configure foreign agents and their security associations.
host1:test(config)#ip mobile secure foreign-agent 100.1.1.3 spi 256 key ascii secret
replay timestamp within 255 algorithm hmac-md5
! Assign an interface profile for the Mobile IP home agent.
host1:test(config)#ip mobile profile testProfile
```

ip mobile home-agent

- Use to configure the Mobile IP home agent on a virtual router.
- To specify the access control list (ACL) applied to the care-of address (CoA) that restricts access for foreign agents or networks, include the **care-of-access** keyword followed by the ACL name.
- To specify the interval within which the registration requests are established, include the **lifetime** keyword followed by the number of seconds, in the range 5–65535; the default value is 36,000 seconds.
- To specify the interval within which a registration can exceed the home agent configured value, include the **replay** keyword followed by the number of seconds, in the range 1–255; the default value is 7 seconds.
- To disable reverse tunneling support by the home agent for denying T bit registration requests, include the **reverse-tunnel-off** keyword; reverse tunneling is enabled by default.
- Example

  ```
  host1(config)#ip mobile home-agent care-of-access acl lifetime 2000 replay 255
  reverse-tunnel-off
  ```

- Use the **no** version to disable the home agent service on the virtual router.

NOTE: The values for lifetime, replay, and care-of-access configured per mobile host by using the **ip mobile host** command override the values configured by using the **ip mobile home-agent** command.

ip mobile host

- Use to configure a mobile node on a virtual router with an optional host network access identifier (NAI) address or the home address (IP address of the home agent).
- To specify the mobile node, include the required **nai** keyword or the required **address** keyword, as follows:
  - To specify the NAI for the mobile node, include the **nai** keyword. You must choose one of the following formats, where *user* represents the user name and *realm* represents the domain name: *user@realm*, *@realm*, or *@*.
  - To specify a nonzero home address of the mobile node, include the **address** keyword followed by the IP address of the mobile node.
- To specify that the AAA server should validate registration requests and obtain configuration and security associations, include the **aaa** keyword.

- To specify the access control list applied to the care-of address that restricts access for foreign agents or networks, include the **care-of-access** keyword followed by the ACL name.
- To specify the interval within which the registration requests are established, include the **lifetime** keyword followed by the number of seconds, in the range 5–65535; the default value is 36,000 seconds.
- Example 1—This example illustrates local authentication of a mobile node; do not specify the **aaa** keyword for local authentication.

  host1(config)#**ip mobile host 200.1.1.1 lifetime 200**

  or

  host1(config)#**ip mobile host nai @amazon.net**

- Example 2—This example illustrates AAA authentication of a mobile node; you must specify the **aaa** keyword for AAA authentication.

  host1(config)#**ip mobile host nai @yahoo.com aaa care-of-access acl2**

  or

  host1(config)#**ip mobile host nai bob@msn.net aaa lifetime 400**

- Use the **no** version to delete the configuration of the mobile node on the virtual router.

ip mobile profile

- Use to configure or associate a preconfigured interface profile with the home agent in a virtual router.
- For information about configuring a virtual router, see the *JUNOSe System Basics Configuration Guide*.
- Example

  host1(config)#**ip mobile profile virDefault**

- Use the **no** version to remove the profile configuration from the virtual router.

ip mobile secure foreign-agent

- Use to configure the security associations for a foreign agent.
- To specify a nonzero address for the foreign agent, include the IP address of the foreign agent.
- To specify the security parameter index (SPI) value to authenticate inbound requests and permit authentication for outbound registration requests, include the required **spi** keyword followed by a 4-octet hexadecimal number, in the range 0x100–0xFFFFFFFF.

- To specify the authentication key for this security association, include the required **key** keyword followed by either the **hex** keyword or the **ascii** keyword, as follows:
  - To specify a hexadecimal key, use the **hex** keyword followed by a 32-character (128-bit) hexadecimal value in the range 0x0–0xFFFFFFFE.
  - To specify an ASCII key, use the **ascii** keyword followed by an alphanumeric value up to a maximum of 16 characters (128 bits).
- To specify the number of seconds by which a registration request can exceed the time value configured on the home agent, include the optional **replay timestamp within** keywords followed by the number of seconds, in the range 1–255; the default value is 7 seconds.
- To specify the type of authentication algorithm for Mobile IP messages, include the optional **algorithm** keyword followed by either the **hmac-md5** keyword or the **keyed-md5** keyword.
- Example

  host1(config)#**ip mobile secure foreign-agent 100.1.1.3 spi 256 key ascii secret replay timestamp within 255 algorithm hmac-md5**

- Use the **no** version to delete the security associations for the specified foreign agent on the virtual router.

ip mobile secure host

- Use to configure the security associations for a mobile node.
- You must configure security associations only for mobile nodes on which local authentication is configured.

NOTE: If you delete a mobile node host by using the **no ip mobile host** command, all security associations that you configured for this host are deleted.

- To specify the mobile node, include the required **nai** keyword or the required **address** keyword, as follows:
  - To specify the network access identifier (NAI) for the mobile node, include the **nai** keyword. You must choose one of the following formats, where *user* represents the user name and *realm* represents the domain name: *user@realm*, *@realm*, or *@*.
  - To specify a nonzero home address of the mobile node, include the **address** keyword followed by the IP address of the mobile node.
- To specify the security parameter index (SPI) value to authenticate inbound requests and permit authentication for outbound registration requests, include the required **spi** keyword followed by a 4-octet hexadecimal number, in the range 0x100–0xFFFFFFFF.

- To specify the authentication key for this security association, include the required **key** keyword followed by either the **hex** keyword or the **ascii** keyword, as follows:
  - To specify a hexadecimal key, use the **hex** keyword followed by a 32-character (128-bit) hexadecimal value in the range 0x0–0xFFFFFFFE.
  - To specify an ASCII key, use the **ascii** keyword followed by an alphanumeric value up to a maximum of 16 characters (128 bits).
- To specify the number of seconds by which a registration request can exceed the time value configured on the home agent, include the optional **replay timestamp within** keywords followed by the number of seconds, in the range 1–255; the default value is 7 seconds.
- To specify the type of authentication algorithm for Mobile IP messages, include the optional **algorithm** keyword followed by either the **hmac-md5** keyword or the **keyed-md5** keyword.
- Examples

  host1(config)#**ip mobile secure host 200.1.1.1 spi 0x398 key ascii w4ex algorithm keyed-md5 replay timestamp within 225**

  or

  host1(config)#**ip mobile secure host nai @amazon.net spi 0x100 key ascii pD4En algorithm keyed-md5 replay timestamp within 100**

- Use the **no** version to delete the security associations for the specified host on the virtual router.

license mobile-ip home-agent

- Use to configure the license key to enable a home agent.
- Specify a name for the license key; up to a maximum of 16 alphanumeric characters.
- Example

  host1(config)#**license mobile-ip home-agent demo**

- Use the **no** version to delete the license key configuration.

Monitoring the Mobile IP Home Agent

Use the commands described in this section to set a statistics baseline, remove the binding table, and verify the configuration of the Mobile IP home agent on a virtual router.

baseline ip mobile home-agent

- Use to set a statistics baseline for a specified Mobile IP home agent.
- Example

  host1#**baseline ip mobile home-agent**

- There is no **no** version.

clear ip mobile binding

- Use to remove the binding table in the specified virtual router or a specified binding by the mobile node home address or NAI.
- Example

  host1#**clear ip mobile binding nai john@yahoo.com**

- There is no **no** version.

show ip mobile binding

- Use to display the binding table information of the home agent in the virtual router.
- Field descriptions
  - MN-NAI—Network access identifier of the mobile node in *user@realm*, *@realm*, or @ format
  - AAA-NAI—Network access identifier returned from the AAA server in *user@realm*, *@realm*, or @ format
  - Home IP address—IP address of the mobile node
  - Home agent address—IP address of the home agent
  - Care-of-address—IP address of the foreign agent care-of address or co-located care-of address
  - Lifetime granted—Interval, in *hh*:*mm*:*sec* format, granted during registration before which the registration request exceeds the home agent configured time
  - Lifetime remaining—Remaining interval, in *hh*:*mm*:*sec* format, at which the registration request exceeds the home agent configured time
  - Tunnel—Configuration information provided while setting up the tunnel between the foreign agent and the home agent
  - Reverse tunnel—Whether reverse tunneling is enabled or disabled
- Example

```
host1#show ip mobile binding
     MN-NAI:  jr@zoom.com
     AAA-NAI: user@zoom.com
     Home IP address:  55.0.0.5
     Home agent address:  66.0.0.5
     Care-of-address:  72.1.1.15
     Lifetime granted :  10:00:00 (36000 seconds)
     Lifetime remaining :  01:46:32
     Tunnel:   Source  66.0.0.5,  Destination 72.1.1.15,  Encapsulation GRE
     Reverse tunnel: enabled
```

show ip mobile home-agent

- Use to display the configuration information of the home agent in the virtual router.
- Field descriptions
  - Access list name—Name of the access control list applied to the care-of address that restricts access for foreign agents or networks
  - Registration lifetime (in seconds)—Number of seconds before which the registration requests are established
  - Replay protection time (in seconds)—Number of seconds before which a registration request can exceed the home agent configured time value
  - Reverse tunnel—Whether reverse tunneling is enabled or disabled
- Example

```
host1#show ip mobile home-agent
Home Agent Parameters
Access list name                        ---
Registration lifetime   (in seconds)    36000
Replay protection time  (in seconds)    7
Reverse tunnel                          enabled
```

show ip mobile host

- Use to display configuration of all or specified mobile nodes or domain users.
- Field descriptions
  - MN-NAI—Network access identifier of the mobile node in *user@realm*, *@realm*, or @ format
  - Home IP address—IP address of the mobile node
  - Lifetime—Number of seconds the registration request is active for a mobile node
  - Care-Of-Access—Name of the ACL applied to the care-of address to restrict network roaming
  - Aaa-Configured—Whether AAA server is configured or not
- Example 1

```
host1#show ip mobile host
                    Home
    MN-NAI        IP address     Lifetime   Care-Of-Access   Aaa-Configured
--------------   -------------   --------   --------------   --------------
@warner.com           ---           36000   ---                    no
@yahoo.com            ---             ---   ---                   yes
pj@juniper.net        ---             100   ---                    no
pm@juniper.net        ---             500   ---                    no
```

- Example 2

```
host1#show ip mobile host nai @warner.com
              Home IP
  MN-NAI      address   Lifetime   Care-Of-Access   Aaa-Configured
-----------   -------   --------   --------------   --------------
@warner.com     ---        36000   ---                    no
```

show ip mobile profile

- Use to display the interface profile name associated with the home agent.
- Field descriptions
  - Mobile IP profile is—Name of the interface profile name associated with the home agent
- Example

```
host1#show ip mobile profile
Mobile IP profile is: mobileIpProfile
```

show ip mobile secure foreign-agent

- Use to display the security associations configured for all foreign agents on the virtual router.
- Field descriptions
  - IP address—IP address of foreign agent
  - SPI—Security parameter index (SPI) key for authenticating registration requests
  - Algorithm—Algorithm (hmac-md5 or keyed-md5) for authenticating Mobile IP messages
  - Replay—Interval, in seconds, before which the registration request exceeds the home agent configured time
  - Key—128-bit hexadecimal number for authenticating the security association.
- Example

```
host1#show ip mobile secure foreign-agent
IP address        SPI         Algorithm   Replay     Key
----------   --------------   ---------   ------   -------
10.10.10.1   628 ( 0x274 )    hmac-md5    ---      secret
20.20.20.1   628 ( 0x274 )    hmac-md5    255      secret
30.30.30.1   628 ( 0x274 )    hmac-md5    255      secret
```

show ip mobile secure host

- Use to display the security associations configured on all mobile node hosts in the virtual router.
- Field descriptions
  - MN-NAI—Network access identifier of the mobile node in *user@realm*, *@realm*, or @ format
  - Home IP address—IP address of the mobile node host
  - SPI—Security parameter index (SPI) key for authenticating registration requests

- Algorithm—Algorithm (hmac-md5 or keyed-md5) for authenticating Mobile IP messages
- Replay—Interval, in seconds, before which the registration request exceeds the home agent configured time
- Key—128-bit hexadecimal number for authenticating the security association

- Example

```
host1#show ip mobile secure host
              Home IP
  MN-NAI      address        SPI          Algorithm   Replay   Key
-----------   -------   --------------   ---------   ------   ----
@warner.com     ---     288 ( 0x120 )    hmac-md5    255      time
```

show ip mobile traffic

- Use to display protocol statistics for the Mobile IP home agent traffic, including advertisements, solicitations, registrations, registration errors, and security violations.
- To display baseline-relative statistics for the Mobile IP home agent traffic, use the optional **delta** keyword.
- Field descriptions
  - Registration requests—Total number of registration requests, de-registration requests, and accepted registration requests for mobile nodes
    - Register—Number of registration requests received by the home agent
    - Deregister—Number of de-registration requests received by the home agent
    - Accept—Number of registration requests accepted by the home agent
  - Registration rejects—Total number of and reasons for unsuccessful responses to registration requests
    - Denied—Number of registration requests denied by the home agent
    - Unspecified—Number of registration requests rejected for an unspecified reason, such as an internal communication failure
    - Unknown HA—Number of registration requests rejected because of an unknown home agent address, or because the specified home agent address is not serviced by this home agent
    - Administratively prohibited—Number of registration requests prohibited for administrative reasons, such as the broadcast or B bit being set without the corresponding D bit, or a denial by the registration filters
    - No Resources—Number of registration requests rejected due to insufficient resources, such as a full binding table, an inability to create a tunnel, or an inability of the IP subscriber management application to create a dynamic subscriber interface
    - Authentication failed MN—Number of registration requests rejected because the mobile node failed authentication

- FA—Number of registration requests rejected because the foreign agent failed authentication
- Bad identification—Number of registration requests rejected because the registration ID field is out of range
- Bad request form—Number of registration requests rejected because of a malformed request
- Unavailable encapsulation—Number of registration requests rejected because of unsupported encapsulation
- No reverse tunnel—Number of registration requests rejected because reverse tunneling is disabled

- Example

```
host1#show ip mobile traffic
Home Agent Registrations:
    Registration requests:
        Register: 0
        Deregister: 0
        Accept: 0

    Registration rejects:
        Denied: 0
        Unspecified: 0
        Unknown HA: 0
        Administratively prohibited: 0
        No Resources: 0
        Authentication failed MN: 0
        FA: 0
        Bad identification: 0
        Bad request form: 0
        Unavailable encapsulation: 0
        No reverse tunnel: 0
```

show license mobile-ip home-agent

- Use to display the license key for the home agent.
- Field descriptions
  - Mobile IP license is—Mobile IP license key associated with the home agent and the maximum number of users allowed by this license
- Example

```
host1#show license mobile-ip home-agent
Mobile IP license is PcZJ93Mt17 which allows 48000 users
```