



Junos[®] OS

Mobile IP Feature Guide for Subscriber Management

Release
13.2



Published: 2013-07-31

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

This product includes the Envoy SNMP Engine, developed by Epilogue Technology, an Integrated Systems Company. Copyright © 1986-1997, Epilogue Technology Corporation. All rights reserved. This program and its documentation were developed at private expense, and no part of them is in the public domain.

This product includes memory allocation software developed by Mark Moraes, copyright © 1988, 1989, 1993, University of Toronto.

This product includes FreeBSD software developed by the University of California, Berkeley, and its contributors. All of the documentation and software included in the 4.4BSD and 4.4BSD-Lite Releases is copyrighted by the Regents of the University of California. Copyright © 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994. The Regents of the University of California. All rights reserved.

GateD software copyright © 1995, the Regents of the University. All rights reserved. Gate Daemon was originated and developed through release 3.0 by Cornell University and its collaborators. Gated is based on Kirton's EGP, UC Berkeley's routing daemon (routed), and DCN's HELLO routing protocol. Development of Gated has been supported in part by the National Science Foundation. Portions of the GateD software copyright © 1988, Regents of the University of California. All rights reserved. Portions of the GateD software copyright © 1991, D. L. S. Associates.

This product includes software developed by Maker Communications, Inc., copyright © 1996, 1997, Maker Communications, Inc.

Juniper Networks, Junos, Steel-Belted Radius, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. The Juniper Networks Logo, the Junos logo, and JunosE are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Products made or sold by Juniper Networks or components thereof might be covered by one or more of the following patents that are owned by or licensed to Juniper Networks: U.S. Patent Nos. 5,473,599, 5,905,725, 5,909,440, 6,192,051, 6,333,650, 6,359,479, 6,406,312, 6,429,706, 6,459,579, 6,493,347, 6,538,518, 6,538,899, 6,552,918, 6,567,902, 6,578,186, and 6,590,785.

Junos® OS Mobile IP Feature Guide for Subscriber Management

13.2

Copyright © 2013, Juniper Networks, Inc.
All rights reserved.

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at <http://www.juniper.net/support/eula.html>. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

	About the Documentation	xi
	Documentation and Release Notes	xi
	Supported Platforms	xi
	Using the Examples in This Manual	xi
	Merging a Full Example	xii
	Merging a Snippet	xii
	Documentation Conventions	xiii
	Documentation Feedback	xv
	Requesting Technical Support	xv
	Self-Help Online Tools and Resources	xv
	Opening a Case with JTAC	xvi
Part 1	Overview	
Chapter 1	Mobile IP in Subscriber Access Networks	3
	Mobile IP Home Agent Elements and Behavior	3
	Mobile IP Registration	6
	Home Address Assignment	6
	Authentication	6
	Reauthentication	7
	AAA Authentication	7
	Local Authentication	8
	Accounting	9
	Mobile IP Routing and Forwarding	10
	Mobile IP in the WiMAX Environment	11
Part 2	Configuration	
Chapter 2	Configuration Overview	17
	Configuring Mobile IP	17
Chapter 3	Configuration Tasks for the Mobile IP Home Agent	19
	Configuring the Mobile IP Authentication Method	19
	Configuring the Mobile IP Home Agent	19
	Configuring the Local Authentication Attributes for the Mobile Node	20
	Configuring Accounting for Mobile IP Subscribers	21
	Configuring Dynamic Home Assignment for the Mobile Node	21
	Configuring the Access Type for Mobile IP	22

Chapter 4	Configuration Statements	23
	[edit services mobile-ip] Hierarchy Level	23
	access-type	24
	algorithm	25
	authenticate	26
	dynamic-home-assignment	27
	enable-service	28
	entity-type	29
	generic	29
	home-agent (Mobile IP Networks)	30
	home-agent (Mobile IP Dynamic Assignment)	31
	home-agent (Mobile IP Network Address Identifier)	32
	home-agent-address	33
	key	34
	mobile-ip	35
	nai	37
	order (Mobile IP)	38
	peer	39
	registration-lifetime	40
	replay-method	41
	revocation-required	42
	spi	43
	statistics (Access Profile)	44
	timestamp-tolerance	45
	traceoptions (Mobile IP)	46
	wimax	48
	virtual-network	49
 Part 3	 Administration	
Chapter 5	Monitoring Commands	53
	clear mobile-ip binding	54
	show mobile-ip home-agent overview	55
	show mobile-ip home-agent bindings	57
	show mobile-ip home-agent traffic	60
	show mobile-ip home-agent virtual-network	63
	show mobile-ip wimax release	65
 Part 4	 Troubleshooting	
Chapter 6	Acquiring Troubleshooting Information	69
	Tracing Mobile IP Operations for Subscriber Access	69
	Configuring the Mobile IP Trace Log Filename	71
	Configuring the Number and Size of Mobile IP Log Files	71
	Configuring Access to the Mobile IP Log File	72
	Configuring a Regular Expression for Mobile IP Messages to Be Logged	72
	Configuring the Mobile IP Tracing Flags	72

	Configuring the Severity Level to Filter Which Mobile IP Messages Are Logged	73
	Collecting Subscriber Access Logs Before Contacting Juniper Technical Support	73
Chapter 7	Troubleshooting Configuration Statement	77
	traceoptions (Mobile IP)	78
Part 5	Index	
	Index	83

List of Figures

Part 1	Overview
Chapter 1	Mobile IP in Subscriber Access Networks 3
	Figure 1: Mobile IP Network Without Reverse Tunneling 4
	Figure 2: Mobile IP Network with Reverse Tunneling 5
	Figure 3: Sample Mobile IP WiMAX Topology 13

List of Tables

	About the Documentation	xi
	Table 1: Notice Icons	xiii
	Table 2: Text and Syntax Conventions	xiii
Part 1	Overview	
Chapter 1	Mobile IP in Subscriber Access Networks	3
	Table 3: Juniper Networks VSAs Used by Mobile IP	7
	Table 4: WiMAX Forum VSAs used by Mobile IP	12
Part 3	Administration	
Chapter 5	Monitoring Commands	53
	Table 5: show mobile-ip home-agent overview Output Fields	55
	Table 6: show mobile-ip home-agent bindings Output Fields	57
	Table 7: show mobile-ip home-agent traffic Output Fields	60
	Table 8: show mobile-ip home-agent virtual-network Output Fields	63
	Table 9: show mobile-ip wimax release Output Fields	65

About the Documentation

- Documentation and Release Notes on page xi
- Supported Platforms on page xi
- Using the Examples in This Manual on page xi
- Documentation Conventions on page xiii
- Documentation Feedback on page xv
- Requesting Technical Support on page xv

Documentation and Release Notes

To obtain the most current version of all Juniper Networks® technical documentation, see the product documentation page on the Juniper Networks website at <http://www.juniper.net/techpubs/>.

If the information in the latest release notes differs from the information in the documentation, follow the product Release Notes.

Juniper Networks Books publishes books by Juniper Networks engineers and subject matter experts. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration. The current list can be viewed at <http://www.juniper.net/books>.

Supported Platforms

For the features described in this document, the following platforms are supported:

- MX Series

Using the Examples in This Manual

If you want to use the examples in this manual, you can use the **load merge** or the **load merge relative** command. These commands cause the software to merge the incoming configuration into the current candidate configuration. The example does not become active until you commit the candidate configuration.

If the example configuration contains the top level of the hierarchy (or multiple hierarchies), the example is a *full example*. In this case, use the **load merge** command.

If the example configuration does not start at the top level of the hierarchy, the example is a *snippet*. In this case, use the **load merge relative** command. These procedures are described in the following sections.

Merging a Full Example

To merge a full example, follow these steps:

1. From the HTML or PDF version of the manual, copy a configuration example into a text file, save the file with a name, and copy the file to a directory on your routing platform.

For example, copy the following configuration to a file and name the file **ex-script.conf**. Copy the **ex-script.conf** file to the **/var/tmp** directory on your routing platform.

```
system {
  scripts {
    commit {
      file ex-script.xml;
    }
  }
}
interfaces {
  fxp0 {
    disable;
    unit 0 {
      family inet {
        address 10.0.0.1/24;
      }
    }
  }
}
```

2. Merge the contents of the file into your routing platform configuration by issuing the **load merge** configuration mode command:

```
[edit]
user@host# load merge /var/tmp/ex-script.conf
load complete
```

Merging a Snippet

To merge a snippet, follow these steps:

1. From the HTML or PDF version of the manual, copy a configuration snippet into a text file, save the file with a name, and copy the file to a directory on your routing platform.

For example, copy the following snippet to a file and name the file **ex-script-snippet.conf**. Copy the **ex-script-snippet.conf** file to the **/var/tmp** directory on your routing platform.

```
commit {
  file ex-script-snippet.xml; }
```

2. Move to the hierarchy level that is relevant for this snippet by issuing the following configuration mode command:

```
[edit]
user@host# edit system scripts
[edit system scripts]
```

3. Merge the contents of the file into your routing platform configuration by issuing the **load merge relative** configuration mode command:

```
[edit system scripts]
user@host# load merge relative /var/tmp/ex-script-snippet.conf
load complete
```

For more information about the **load** command, see the *CLI User Guide*.

Documentation Conventions

Table 1 on page xiii defines notice icons used in this guide.

Table 1: Notice Icons


Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.

Table 2 on page xiii defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the configure command: user@host> configure
Fixed-width text like this	Represents output that appears on the terminal screen.	user@host> show chassis alarms No alarms currently active

Table 2: Text and Syntax Conventions (*continued*)

Convention	Description	Examples
<i>Italic text like this</i>	<ul style="list-style-type: none"> Introduces or emphasizes important new terms. Identifies book names. Identifies RFC and Internet draft titles. 	<ul style="list-style-type: none"> A policy <i>term</i> is a named structure that defines match conditions and actions. <i>Junos OS System Basics Configuration Guide</i> RFC 1997, <i>BGP Communities Attribute</i>
<i>Italic text like this</i>	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# set system domain-name <i>domain-name</i>
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	<ul style="list-style-type: none"> To configure a stub area, include the stub statement at the [edit protocols ospf area area-id] hierarchy level. The console port is labeled CONSOLE.
< > (angle brackets)	Enclose optional keywords or variables.	stub <default-metric <i>metric</i> >;
(pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	broadcast multicast (<i>string1</i> <i>string2</i> <i>string3</i>)
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	rsvp { # Required for dynamic MPLS only
[] (square brackets)	Enclose a variable for which you can substitute one or more values.	community name members [<i>community-ids</i>]
Indentation and braces ({ })	Identify a level in the configuration hierarchy.	[edit] routing-options { static { route default { nexthop <i>address</i> ; retain; } } }
;(semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
GUI Conventions		
Bold text like this	Represents graphical user interface (GUI) items you click or select.	<ul style="list-style-type: none"> In the Logical Interfaces box, select All Interfaces. To cancel the configuration, click Cancel.
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select Protocols>Ospf .

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can send your comments to techpubs-comments@juniper.net, or fill out the documentation feedback form at <https://www.juniper.net/cgi-bin/docbugreport/>. If you are using e-mail, be sure to include the following information with your comments:

- Document or topic name
- URL or page number
- Software release version (if applicable)

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at <http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf>.
- Product warranties—For product warranty information, visit <http://www.juniper.net/support/warranty/>.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: <http://www.juniper.net/customers/support/>
- Search for known bugs: <http://www2.juniper.net/kb/>
- Find product documentation: <http://www.juniper.net/techpubs/>
- Find solutions and answer questions using our Knowledge Base: <http://kb.juniper.net/>
- Download the latest versions of software and review release notes: <http://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications: <https://www.juniper.net/alerts/>

- Join and participate in the Juniper Networks Community Forum:
<http://www.juniper.net/company/communities/>
- Open a case online in the CSC Case Management tool: <http://www.juniper.net/cm/>

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: <https://tools.juniper.net/SerialNumberEntitlementSearch/>

Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at <http://www.juniper.net/cm/>.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see <http://www.juniper.net/support/requesting-support.html>.

PART 1

Overview

- [Mobile IP in Subscriber Access Networks on page 3](#)

CHAPTER 1

Mobile IP in Subscriber Access Networks

- [Mobile IP Home Agent Elements and Behavior on page 3](#)
- [Mobile IP Registration on page 6](#)
- [Mobile IP Routing and Forwarding on page 10](#)
- [Mobile IP in the WiMAX Environment on page 11](#)

Mobile IP Home Agent Elements and Behavior

Mobile IP is a tunneling-based solution that enhances the utility of Junos routing platforms 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.

You configure Mobile IP home agent parameters in the **[edit services mobile-ip]** hierarchy level, the **[edit logical-systems *logical-system-name*]** hierarchy level, and the **[edit routing-instances *routing-instances-name*]** hierarchy level.



NOTE: Currently, Junos OS does not support configuration of the Mobile IP foreign agent.

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.

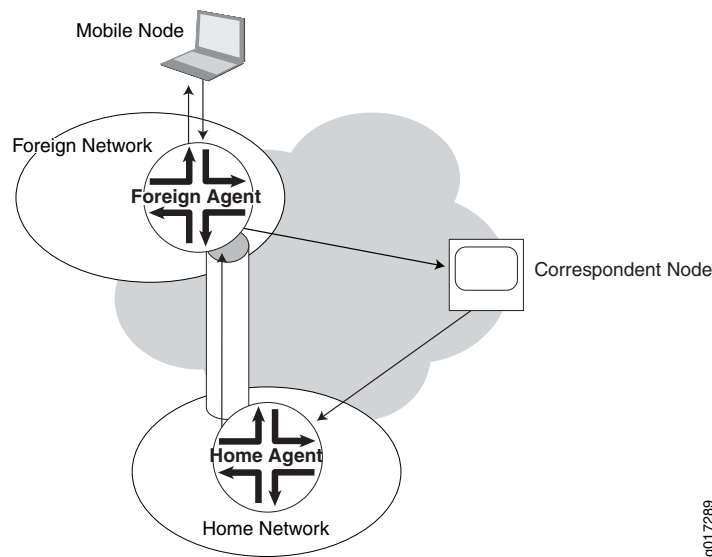
When a mobile node roams into a new, foreign network, it negotiates with the foreign agent to get a secondary IP address, which is referred to as the care-of address. The mobile node registers this care-of address with the home agent. The home agent then establishes a tunnel to the care-of address if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



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

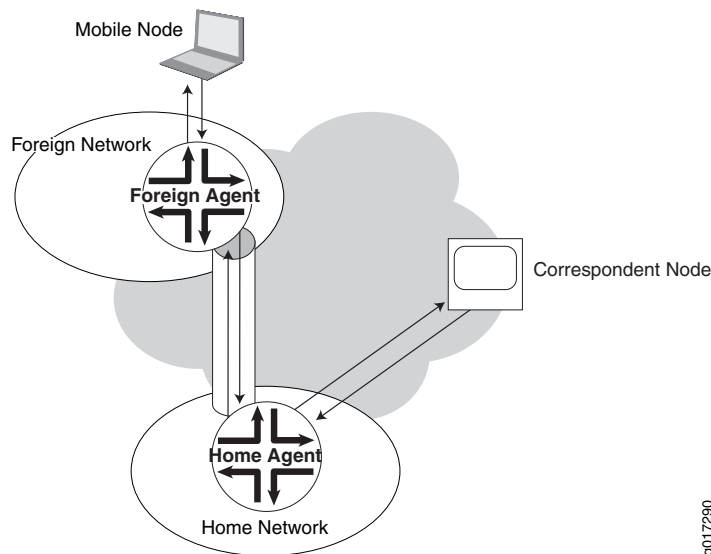
Packets sent to the home address of the mobile node are redirected by the home agent through the tunnel to the care-of address at the foreign agent. The foreign agent routes the packets to the mobile node's home address. [Figure 1 on page 4](#) illustrates this forwarding and routing process behavior. Although the traffic to the correspondent node comes from the foreign agent, to the correspondent node the traffic appears to come from the mobile node's home network.

Figure 1: Mobile IP Network Without Reverse Tunneling



If the mobile node's home address is a private address or if the foreign agent implements ingress filtering, a reverse tunnel from the care-of address to the home agent is required. This reverse tunnel capability is negotiated between the foreign agent and the home agent when the mobile node requests registration. Traffic from a correspondent node to the mobile node is forwarded by the home agent through the foreign agent as in the other scenario. [Figure 2 on page 5](#) shows how traffic from the mobile node to a correspondent node is tunneled from the foreign agent to the home agent and then routed to the correspondent node by the home agent.

Figure 2: Mobile IP Network with Reverse Tunneling



Mobile nodes typically belong to a virtual network, which is an address range or subnet that is not directly served by any physical, routed interface on the home network. These mobile nodes never return home to attach to a physical interface on the home agent. Traffic destined for the mobile node can be forwarded over any interface.

You can use the Mobile IP home agent feature to configure the home agent within the default router context with either local or AAA authentication. When you configure local authentication, you can also configure Mobile IP independently in any named routing instance in any configured logical router. When you configure AAA as the authentication method, you can configure Mobile IP only in the default router context.

The Mobile IP home agent can also receive, process, and send Worldwide Interoperability for Microwave Access (WiMAX) vendor-specific RADIUS attributes (VSAs). This feature enables Mobile IP home agent to work in a WiMAX home connectivity services network (H-CSN), to provide for mobility management at the IP layer.

The home agent handles the following tasks:

- Registration of mobile nodes
- Routing and forwarding of mobile node traffic

Related Documentation

- [Mobile IP Registration on page 6](#)
- [Mobile IP Routing and Forwarding on page 10](#)
- [Mobile IP in the WiMAX Environment on page 11](#)
- [Configuring Mobile IP on page 17](#)

Mobile IP Registration

The home agent receives the registration requests (RRQs) on UDP port 434. The registration request contains the home agent IP address. The home agent can support static home address allocation and dynamic home address allocation. The home agent can revoke a mobile node's registration. When this happens, the mobility binding is removed and the foreign agent is informed of the revocation so it can free up its resources. The foreign agent can send a registration revocation request to the home agent when the mobile node roams to another area. The revocation request can include a revocation support extension to indicate that it supports the revocation mechanism.

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 and NAI (if the NAI is present).

If the home address is dynamically allocated, the mobile node submits a zero 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 authentication, authorization, and accounting (AAA) server back-end address mechanisms, such as:

- By RADIUS, in the Framed-IP-Address attribute
- From a local address pool returned by RADIUS in the Framed-Pool attribute

Authentication

The home agent authenticates the requests based on RFC 3344—IP Mobility Support for IPv4 (August 2002). By default, a AAA server is used for authentication; alternatively, you can configure local authentication parameters on the home agent. The mobile node 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 the 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 authenticator, the mobile-home extension is authenticated. For local authentication, the key is limited to a maximum of 128 bits. For AAA authentication, the key can be longer depending on the maximum length configured on the AAA server.

When HA receives the access accept from the AAA, it extracts the MN-HA key from the response. The home agent does the MN-HA authentication extension processing based on the MN-HA key by running authentication algorithm (HMAC-MD5 or Keyed-MD5) on the message to compute a hash (authenticator), which is compared with the hash value in the MN-HA extension. If the hash value matches, the RRQ is considered 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 to verify that a registration message has been freshly generated by the mobile node, and is not simply being replayed by an attacker from some previous registration. The ID field represents a 64-bit Network Time Protocol (NTP)-formatted time value. The configured replay timestamp defines the tolerance time window in seconds by which a registration request timestamp and the local time of the HA can differ. By default, the timestamp must be within 7 seconds of the replay tolerance configured for the mobile node or, if that is configured, the timestamp tolerance of the home agent itself.

Reauthentication

Reauthentication is not currently supported by the authentication process. Mobile IP caches a security association for each mobile node, which helps overcome this limitation. When a mobile node requests re-registration or de-registration, Mobile IP refers to the cached security association for that mobile node and performs MD5 message authentication.

When the security association for the mobile node changes after the node is authenticated, the cache entry is not invalidated. Consequently, the mobile node's RRQ is rejected. In this case you must clear the binding with the mobile node so that it can de-register and then log in.

RADIUS server configuration changes relating to the subscriber do not propagate to the cache. In this case you must clear the binding with the mobile node so that it can de-register and then log in.

AAA Authentication

You can store the security associations and configuration information remotely on a RADIUS server. The home agent applies the authentication algorithm and security key to the mobile node's message. The AAA server uses Juniper Networks vendor-specific attributes (VSAs; vendor ID 4874) listed in [Table 3 on page 7](#). These VSAs are mandatory in the reply to provide the appropriate authentication algorithm and the secure key for the authentication request. If the 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.

Table 3: Juniper Networks VSAs Used by Mobile IP

Attribute Number	Attribute Name	Description	Value
26–84	Mobile-IP-Algorithm	Authentication algorithm used for Mobile-IP registration	integer: 4-octet
26–85	Mobile-IP-SPI	Security parameter index for Mobile IP registration	integer: 4-octet

Table 3: Juniper Networks VSAs Used by Mobile IP (*continued*)

Attribute Number	Attribute Name	Description	Value
26–86	Mobile-IP-Key	Security association MD5 key for Mobile IP registration	string: key
26–87	Mobile-IP-Replay	Replay timestamp for Mobile IP registration	integer: 4-octet
26–89	Mobile-IP-Lifetime	Registration lifetime for Mobile IP registration	integer: 4-octet

AAA authentication is accomplished by generating a AAA access-request to a AAA server. This is the default authentication mode, but you can include the **authenticate order aaa** statement at the **[edit services mobile-ip]** hierarchy level to explicitly configure AAA authentication. You cannot configure a fallback mechanism for AAA authentication. If the AAA request times out, the home agent does not fall back on the local router to determine the authentication parameters. The registration request is rejected. When the message is authenticated, the AAA server always returns either the Framed-IP-Address or Framed-Pool attribute for the user.

The presence of the mobile node's NAI and home IP address in the authentication request that the home agent sends to the AAA server is determined by their presence in the mobile node RRQ received by the home agent:

- When both the NAI and home 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.
- When only the NAI is present in the registration request, then the NAI is used as the user name.
- When only the IP address (home address) is present in the registration request, then the IP address is used as the user name.
- When both the NAI address and the IP address are missing from the registration request, then the registration request is rejected.

Local Authentication

As an alternative to the default authentication by AAA server, you can store the security associations and configuration information locally on the router hosting the home agent. Local authentication is accomplished by querying the locally configured security parameters for the mobile node. The home agent applies the authentication algorithm and security key to the mobile node's message. If the security parameters are not available or do not match the RRQ, then the request for mobility service is rejected, a security violation error is logged, and no registration reply is generated.

For local authentication, include the **authenticate order local** statement at the **[edit services mobile-ip]** hierarchy level. You cannot configure a fallback mechanism for local

authentication. If the local authentication fails, the home agent does not fall back on the AAA server to determine the authentication parameters. The registration request is rejected. Include the **peer** statement at the **[edit services mobile-ip]** hierarchy level to configure the authentication attributes on the home agent for a user identified by IP address or network address identifier (NAI). This user can be a mobile node or a foreign agent.

The authentication attributes include a security parameter index (SPI) to identify a particular security context between the home agent and the mobile node or foreign agent among the contexts available in the mobility security association. Associated with each SPI is the MD5 algorithm and key used to authenticate messages from the mobile node or foreign agent. You can also configure the replay timestamp tolerance for the mobile node or foreign agent.

When local authentication is configured, you can configure Mobile IP independently in any named routing instance in any configured logical router. All Mobile IP statements are available in those contexts, except for the **order aaa** statement at the **[edit services mobile-ip authenticate]** hierarchy level.

Accounting

The Junos Mobile IP home agent application supports time-based accounting for Mobile IP subscribers. Include the **statistics time** statement in the subscriber access profile at the **[edit access profile profile-name accounting]** hierarchy level. Time-based accounting for Mobile IP subscribers also requires that you include the **authenticate order aaa** statement at the **[edit services mobile-ip]** hierarchy level. Accounting begins when the Mobile IP home agent registers the mobile node and creates a binding with the mobile node.

Accounting stops when the binding is deleted. Any of the following actions can cause the binding to be deleted:

- The mobile user logs off.
- The binding lifetime expires.
- The mobile node is deregistered for any reason.
- The foreign agent sends a revocation message.

The Acct-Start message the home agent sends to the AAA server includes the network address identifier (NAI) in the User-Name attribute and the home address of the mobile IP node in the Framed-IP-Address attribute. The Acct-Stop message additionally includes the Acct-Session-Id and Acct-Session-Time attributes.

You cannot currently configure time-based accounting for only the Mobile IP service in a given logical router or routing instance. Enabling time-based accounting for Mobile IP also enables time-based accounting for all other services that are configured in that logical router or routing instance. If you do not want time-based accounting to apply to other services, then you must configure those services in a different logical router or routing instance.

- Related Documentation**
- For information about the specific Juniper Networks VSAs used for Mobile IP RADIUS-based authentication, see *Juniper Networks VSAs Supported by the AAA Service Framework*
 - [Mobile IP Home Agent Elements and Behavior on page 3](#)
 - [Mobile IP Routing and Forwarding on page 10](#)
 - [Mobile IP in the WiMAX Environment on page 11](#)
 - [Configuring Mobile IP on page 17](#)

Mobile IP Routing and Forwarding

Mobile IP employs a care-of address to process traffic for the mobile node.

The mobile node acquires the a care-of address from the foreign agent. The care-of address is reachable from the mobile node, and routable from the home agent. The mobile node includes the care-of address in its registration request to the home agent. After AAA or local authentication successfully processes and authenticates the RRQ and provides both the authorization parameters for the mobile node and an IP address, the home agent then sets up the data path for the mobile node and sends back a registration reply (RRP) confirming successful registration of the mobile node.

When the foreign agent receives the successful RRP from the home agent, the foreign agent sets up the data path for the mobile node. Then it sends the RRP to the mobile node to acknowledge that the mobile node is now successfully registered and the data path between the home agent and the mobile node is in place.

The home agent supports generic routing encapsulation (GRE) and IP-in-IP tunnel encapsulation for forward and reverse tunneling. The tunnels must be statically configured. When packets destined for the mobile node reach a home agent, the home agent encapsulates the packets and tunnels them to the care-of address. 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.

Mobile IP does not support graceful Routing Engine switchover (GRES). It handles the rebooting of processes in the following ways:

- Mobile IP process—After Mobile IP completes a restart, it removes the Mobile IP subscriber entries from AAA and the session database. When that is complete, Mobile IP can process new mobile node registration requests.
- AAA process—After AAA completes a restart, Mobile IP removes all subscriber data held internally by AAA and all corresponding session database entries.
- Routing protocol process—When the connection between the routing protocol process and Mobile IP is lost, Mobile IP responds by clearing the mobile node bindings that are associated with the logical system in which the routing protocol process restarted. The

routing protocol process maintains routes to mobile nodes during the restart. The routing protocol process flushes these routes if they are not reinstalled after the restart completes and before the stale route timer expires.

- Related Documentation**
- [Mobile IP Home Agent Elements and Behavior on page 3](#)
 - [Mobile IP Registration on page 6](#)
 - [Mobile IP in the WiMAX Environment on page 11](#)
 - [Configuring Mobile IP on page 17](#)

Mobile IP in the WiMAX Environment

Worldwide Interoperability for Microwave Access (WiMAX) is the international standard for wide area radio access networks. It provides a framework for networks that are implemented in different ways to successfully interoperate with mobile subscribers that roam among the networks. This interoperability enables the subscribers to be authenticated by their home network wherever they roam, and to receive the services for which they are authorized.

The Mobile IP home agent can operate in either of two access modes, generic and WiMAX. The generic access type is appropriate when the home agent is deployed in a generic Mobile IP home network. When deployed as a home agent in a WiMAX home connectivity services network (H-CSN), you must configure the WiMAX access type. The WiMAX access type enables the Mobile IP home agent to receive, process, and send WiMAX vendor-specific attributes (VSAs) that are used by AAA and the RADIUS server to authenticate the mobile subscriber. When the access type is generic, the Mobile IP home agent cannot handle these VSAs.



NOTE: The Mobile IP configuration for WiMAX requires that AAA be used for the authentication method. For that reason, WiMAX is available only in the default router context.

A WiMAX H-CSN is analogous to the Mobile IP home network for non-WiMAX implementations. When WiMAX is enabled for the Mobile IP home agent in an H-CSN, the Mobile IP home agent triggers subscriber authentication when the agent receives the registration request. The home agent stores WiMAX Forum (vendor ID 24757) vendor-specific attributes (VSAs) listed in [Table 4 on page 12](#) in the session database based on the registration request.

Table 4: WiMAX Forum VSAs used by Mobile IP

Attribute Number	Attribute Name	Description	Value
26-1	WiMAX-Capability	Identifies the WiMAX capabilities supported by the home agent (sent in the Access-Request message). In an Access-Accept message, identifies the capabilities selected by the RADIUS server (returned in the Access-Accept message).	string or integer
26-6	hHA-IP-MIP4	IP address of the home agent (hHA) making the request	octet string: IP address
26-10	MN-HA-MIP4-KEY	MN-hHA key sent by the RADIUS server for validation by the home agent	integer: 2-octet salt followed by 16-octet encrypted MN-hHA hash key
26-11	MN-HA-MIP4-SPI	Security parameter index (SPI) associated with the MN-HA-MIP4 key	integer: 4-octet
26-15	hHA-RK-KEY	Key used by the NAS to generate FA-HA keys	integer: 2-octet salt followed by 16-octet encrypted MN-hHA hash key
26-16	hHA-RK-SPI	SPI associated with the hHA-RK key	integer: 4-octet
26-17	HA-RK-Lifetime	Lifetime of the hHA-RK key and derived keys	integer: 4-octet
26-18	RRQ-HA-IP	IP address of the home agent contained in the Mobile IP registration request or the binding update	octet string: IP address

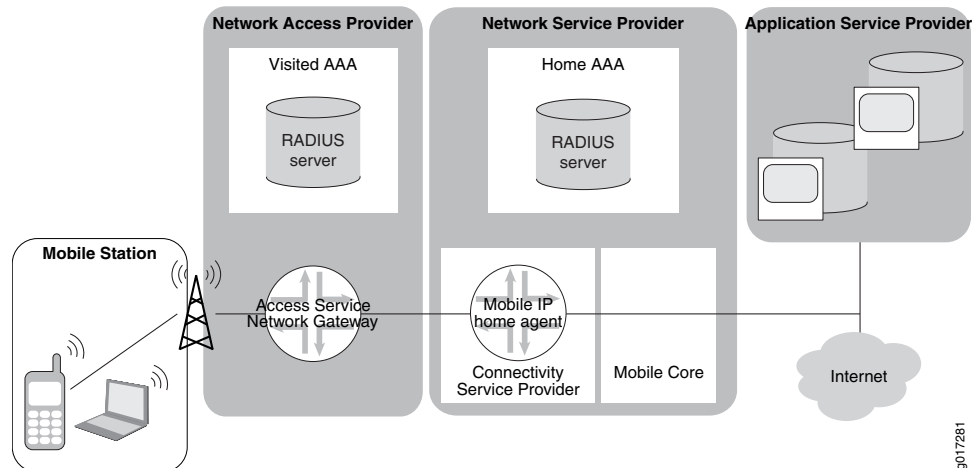
Table 4: WiMAX Forum VSAs used by Mobile IP (*continued*)

Attribute Number	Attribute Name	Description	Value
26–19	RRQ-MN-HA-KEY	The MN-HA key bound to the home agent IP address as reported by the RRQ-HA-IP attribute. Used to validate the MN-HA-AE of the Mobile IP registration request.	integer: 2-octet salt followed by 16-octet encrypted MN-hHA hash key

The home agent requests AAA to fetch the corresponding WiMAX-related information from the RADIUS server. The AAA client sends an Access-Request message to the server. The RADIUS server responds with the necessary WiMAX information, such as the MN-HA key and the HA-RK key, and then the AAA client passes the response to the home agent. The Mobile IP home agent verifies the response received from AAA, processes the registration request, and then grants, extends, or denies subscriber registration.

Figure 3 on page 13 shows the elements of a sample WiMAX topology.

Figure 3: Sample Mobile IP WiMAX Topology



The Mobile IP subscriber registration flow is a four-step process.

1. The access service network gateway (ASN-GW) sends the subscriber registration request from the mobile node to the Mobile IP home agent. The registration request is protected by the MN-HA authentication extension and the FA-HA authentication extension.
2. The home agent requests that the RADIUS server send the cryptographic keys for the Mobile IP session identified by user@realm. The home agent notifies the RADIUS server that it seeks to source IP session-based accounting messages.

3. The RADIUS server agrees to use IP session-based accounting, provides the requested cryptographic keys, and sends the AAA-Session-ID for this session.
4. The home agent replies to the Mobile IP registration request.

Reauthentication of WiMAX subscribers is not currently supported.

You can configure the Mobile IP home agent for WiMAX access by including the **wimax** statement at the **[edit services mobile-ip access-type]** hierarchy level. You can prevent the Mobile IP home agent from being able to process WiMAX VSAs by either removing the **wimax** statement at the **[edit services mobile-ip access-type]** hierarchy level or by including the **generic** statement at the **[edit services mobile-ip access-type]** hierarchy level. The default access type for Mobile IP home agent is generic.

**Related
Documentation**

- For information about the specific Juniper Networks VSAs used for Mobile IP RADIUS-based authentication, see *Juniper Networks VSAs Supported by the AAA Service Framework*
- [Mobile IP Home Agent Elements and Behavior on page 3](#)
- [Mobile IP Registration on page 6](#)
- [Mobile IP Routing and Forwarding on page 10](#)
- [Configuring Mobile IP on page 17](#)

PART 2

Configuration

- [Configuration Overview on page 17](#)
- [Configuration Tasks for the Mobile IP Home Agent on page 19](#)
- [Configuration Statements on page 23](#)

CHAPTER 2

Configuration Overview

- [Configuring Mobile IP on page 17](#)

Configuring Mobile IP

You can configure Mobile IP to provide mobility for subscribers in IP networks. The Mobile IP home agent authenticates registration requests from mobile users and forward traffic to them at their care-of address without having to advertise that address to the wider network.

To configure Mobile IP for mobile subscriber access:

1. Configure the authentication method for registration requests, local or AAA.
See [“Configuring the Mobile IP Authentication Method” on page 19](#).
2. Configure the Mobile IP home agent.
See [“Configuring the Mobile IP Home Agent” on page 19](#).
3. Configure the authentication attributes for the mobile node.
See [“Configuring the Local Authentication Attributes for the Mobile Node” on page 20](#).
4. Configure accounting for Mobile IP subscribers.
See [“Configuring Accounting for Mobile IP Subscribers” on page 21](#).
5. Configure the dynamic reassignment of the mobile node to another home agent.
See [“Configuring Dynamic Home Assignment for the Mobile Node” on page 21](#).
6. Configure the access type for Mobile IP.
See [“Configuring the Access Type for Mobile IP” on page 22](#).
7. Configure trace options for troubleshooting the configuration.
See [“Tracing Mobile IP Operations for Subscriber Access” on page 69](#).

CHAPTER 3

Configuration Tasks for the Mobile IP Home Agent

- [Configuring the Mobile IP Authentication Method on page 19](#)
- [Configuring the Mobile IP Home Agent on page 19](#)
- [Configuring the Local Authentication Attributes for the Mobile Node on page 20](#)
- [Configuring Accounting for Mobile IP Subscribers on page 21](#)
- [Configuring Dynamic Home Assignment for the Mobile Node on page 21](#)
- [Configuring the Access Type for Mobile IP on page 22](#)

Configuring the Mobile IP Authentication Method

You can configure Mobile IP to authenticate registration requests from mobile nodes by either the locally configured attributes or a AAA server. AAA server authentication is the default method.



NOTE: AAA server authentication is available only in the default router context. Local authentication is available in both default and nondefault router contexts.

To configure the Mobile IP authentication method:

- Specify either local or AAA authentication.

```
[edit services mobile-ip]  
user@host# set authenticate order local
```

Related Documentation

- [Configuring Mobile IP on page 17](#)

Configuring the Mobile IP Home Agent

To configure the home agent for a Mobile IP virtual network:

1. Configure the loopback IP address that is used as the home agent IP address.

```
[edit services mobile-ip home-agent virtual-network]
user@host# set home-agent-address 10.5.5.0
```

2. (Optional) Configure the maximum lifetime that the home agent accepts in any registration request from a mobile node.

```
[edit services mobile-ip home-agent virtual-network]
user@host# set home-agent-address 10.5.5.0 registration-lifetime 100
```

3. (Optional) Configure a timestamp tolerance for registration replay protection.

```
[edit services mobile-ip home-agent virtual-network]
user@host# set home-agent-address 10.5.5.0 timestamp-tolerance 200
```

4. Configure whether the home agent can revoke a mobile node's registration to deactivate the node.

```
[edit services mobile-ip home-agent virtual-network]
user@host# set home-agent-address 10.5.5.0 revocation-required
```

5. Specify the interfaces on which the home agent accepts registration requests.

```
[edit services mobile-ip home-agent]
user@host# set enable-service ge-0/0/1.0
user@host# set enable-service ge-0/0/2.0
user@host# set enable-service ge-0/0/3.0
user@host# set enable-service ge-0/0/4.0
```

Related Documentation • [Configuring Mobile IP on page 17](#)

Configuring the Local Authentication Attributes for the Mobile Node

You specify for each mobile node several attributes that enable authentication of registration requests from the node. These attributes include security association context for the peering relationship, the entity type of the node, the encryption algorithm and key used to authenticate the request, and replay protection.

To configure authentication attributes for the mobile node:

1. Configure the peer entity for the security parameter.

```
[edit services mobile-ip]
user@host# set peer ip-address 10.4.2.20 spi 500 entity-type mobility-agent
```

2. Configure the algorithm used for authenticating Mobile IP messages. By default, the hmac-md5 algorithm is used.

```
[edit services mobile-ip]
user@host# set peer ip-address 10.4.2.20 spi 500 algorithm md5
```

3. Configure the authentication key for the security association, in either HEX or ASCII format.

```
[edit services mobile-ip]
user@host# set peer ip-address 10.4.2.20 spi 500 key ascii xf125j9m
```

4. Configure a timestamp tolerance for registration replay protection or specify that the timestamp tolerance be taken from the value configured on the home agent.

```
[edit services mobile-ip]
user@host# set peer ip-address 10.4.2.20 spi 500 replay-method timestamp tolerance
250
```

Related Documentation

- [Configuring Mobile IP on page 17](#)

Configuring Accounting for Mobile IP Subscribers

You can configure time-based accounting to track the subscriber sessions of Mobile IP subscribers.

To configure Mobile IP accounting:

1. Configure the IP address for the RADIUS accounting server.

```
[edit access profile mip-win4]
user@host# set radius accounting-server 192.168.20.5
```

2. Specify RADIUS as the accounting method for Mobile IP subscribers.

```
[edit access profile mip-win4 accounting]
user@host# set order radius
```

3. Specify time-based accounting for the access profile used for the subscriber.

```
[edit access profile mip-win4 accounting]
user@host# set statistics time
```

Related Documentation

- [Configuring Mobile IP on page 17](#)
- *Specifying the Authentication and Accounting Methods for Subscriber Access*
- *Configuring Per-Subscriber Session Accounting*
- *Configuring RADIUS Server Parameters for Subscriber Access*

Configuring Dynamic Home Assignment for the Mobile Node

The mobile node can request that the home agent dynamically assign an IP address for the home agent. The mobile node uses this address for the home agent in all subsequent registration requests until the registration expires or the mobile node is rebooted.

To configure the IP address to be used by the mobile node for the home agent:

- Configure the IP address for the specified mobile node.

```
[edit services mobile-ip]
user@host# set dynamic-home-assignment home-agent nai bws@example.com
home-agent 192.168.4.5
```

Related Documentation

- [Configuring Mobile IP on page 17](#)

Configuring the Access Type for Mobile IP

You can configure the Mobile IP home agent to operate in a Worldwide Interoperability for Microwave Access (WiMAX) home connectivity services network (H-CSN). This configuration enables the home agent to receive, process, and send WiMAX VSAs for subscriber authentication and registration. By default, Mobile IP cannot process the WiMAX VSAs. For operation in non-WiMAX environments, you can return it to this mode by configuring the **generic** access type.



NOTE: The Mobile IP configuration for WiMAX requires that AAA be used for the authentication method. For that reason, WiMAX is available only in the default router context.

To configure the access type, do one of the following:

- Configure generic operation.

```
[edit services mobile-ip]  
user@host# set access-type generic
```
- Configure WiMAX operation.

```
[edit services mobile-ip]  
user@host# set access-type wimax
```

Related Documentation

- [Configuring Mobile IP on page 17](#)

CHAPTER 4

Configuration Statements

- [\[edit services mobile-ip\] Hierarchy Level on page 23](#)

[\[edit services mobile-ip\] Hierarchy Level](#)

```
services {
  mobile-ip {
    access-type {
      (generic | wimax);
    }
    authenticate {
      order (aaa | local);
    }
    dynamic-home-assignment {
      home-agent {
        nai (name@domain | @domain) {
          home-agent ip-address;
        }
      }
    }
    home-agent {
      enable-service interface-name;
      virtual-network {
        home-agent-address ip-address {
          registration-lifetime seconds;
          revocation-required;
          timestamp-tolerance seconds;
        }
      }
    }
  }
  peer {
    (ip-address address | nai name@domain) {
      spi hexadecimal-value {
        algorithm (hmac-md5 | md5);
        entity-type (host | mobility-agent);
        key (hex | ascii) string;
        replay-method (none | timestamp seconds);
      }
    }
  }
  traceoptions {
```

```
file filename <files number> <match regular-expression > <size maximum-file-size>
    <world-readable | no-world-readable>;
flag flag;
level <all | error | info | notice | verbose | warning>;
no-remote-trace;
}
}
}
```

- Related Documentation**
- [Mobile IP Home Agent Elements and Behavior on page 3](#)
 - [Configuring Mobile IP on page 17](#)

access-type

Syntax	<pre>access-type { (generic wimax); }</pre>
Hierarchy Level	<pre>[edit services mobile-ip], [edit logical-systems <i>logical-system-name</i> services mobile-ip], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> services mobile-ip], [edit routing-instances <i>routing-instance-name</i> services mobile-ip]</pre>
Release Information	Statement introduced in Junos OS Release 9.5.
Description	<p>Configure the access type for Mobile IP.</p> <p>The remaining statements are explained separately.</p>
Default	The generic access type is used by default.
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• Configuring Mobile IP on page 17• Configuring the Access Type for Mobile IP on page 22

algorithm

Syntax	algorithm (hmac-md5 md5);
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> services mobile-ip peer ip-address <i>address</i> spi <i>hexadecimal-value</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> services mobile-ip peer nai <i>user@domain</i> spi <i>hexadecimal-value</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> services mobile-ip peer ip-address <i>address</i> spi <i>hexadecimal-value</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> services mobile-ip peer nai <i>user@domain</i> spi <i>hexadecimal-value</i>],</p> <p>[edit routing-instances <i>routing-instances-name</i> services mobile-ip peer ip-address <i>address</i> spi <i>hexadecimal-value</i>],</p> <p>[edit routing-instances <i>routing-instances-name</i> services mobile-ip peer nai <i>user@domain</i> spi <i>hexadecimal-value</i>],</p> <p>[edit services mobile-ip peer ip-address <i>address</i> spi <i>hexadecimal-value</i>],</p> <p>[edit services mobile-ip peer nai <i>user@domain</i> spi <i>hexadecimal-value</i>]</p>
Release Information	<p>Statement introduced in Junos OS Release 9.3.</p> <p>Support at the [edit logical-systems <i>logical-system-name</i> ...], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> ...], and [edit routing-instances <i>routing-instances-name</i> ...] hierarchy levels introduced in Junos OS Release 9.5.</p>
Description	Configure the algorithm used for authenticating Mobile IP messages.
Default	hmac-md5
Options	<p>hmac-md5—Specifies algorithm hmac-md5</p> <p>md5—Specifies algorithm md5</p>
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Mobile IP on page 17 • Configuring the Mobile IP Home Agent on page 19

authenticate

Syntax	<pre>authenticate { order (aaa local); }</pre>
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> services mobile-ip], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> services mobile-ip], [edit routing-instances <i>routing-instances-name</i> services mobile-ip], [edit services mobile-ip]
Release Information	Statement introduced in Junos OS Release 9.3. Support at the [edit logical-systems <i>logical-system-name</i> ...], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> ...], and [edit routing-instances <i>routing-instances-name</i> ...] hierarchy levels introduced in Junos OS Release 9.5.
Description	Define the authentication method performed for Mobile IP. The remaining statement is explained separately.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Mobile IP on page 17• Configuring the Access Type for Mobile IP on page 22

dynamic-home-assignment

Syntax	<pre>dynamic-home-assignment { home-agent { nai (name@domain.com @domain.com) { home-agent ip-address; } } }</pre>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> services mobile-ip], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> services mobile-ip], [edit routing-instances <i>routing-instances-name</i> services mobile-ip], [edit services mobile-ip]</p>
Release Information	<p>Statement introduced in Junos OS Release 9.3. Support at the [edit logical-systems <i>logical-system-name</i> ...], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> ...], and [edit routing-instances <i>routing-instances-name</i> ...] hierarchy levels introduced in Junos OS Release 9.5.</p>
Description	<p>Define the dynamic assignment rule for the home agent.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>system—To view this statement in the configuration. system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Mobile IP on page 17 • Configuring Dynamic Home Assignment for the Mobile Node on page 21

enable-service

Syntax	<code>enable-service <i>interface-name</i>;</code>
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> services mobile-ip home-agent], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> services mobile-ip home-agent], [edit routing-instances <i>routing-instances-name</i> services mobile-ip home-agent], [edit services mobile-ip home-agent]
Release Information	Statement introduced in Junos OS Release 9.3. Support at the [edit logical-systems <i>logical-system-name</i> ...], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> ...], and [edit routing-instances <i>routing-instances-name</i> ...] hierarchy levels introduced in Junos OS Release 9.5.
Description	Define the list of interfaces on which the home agent service can be enabled. The system accepts registration requests only if it is on one of these interfaces. Include the statement once for each interface to be enabled.
Options	<i>interface-name</i> —Interface on which the home agent can be enabled.
Required Privilege Level	view—To view this statement in the configuration. view-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Mobile IP on page 17• Configuring the Mobile IP Home Agent on page 19

entity-type

Syntax	entity-type (host mobility-agent);
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> services mobile-ip peer spi <i>hexadecimal-value</i>], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> services mobile-ip peer spi <i>hexadecimal-value</i>], [edit routing-instances <i>routing-instances-name</i> services mobile-ip peer spi <i>hexadecimal-value</i>], [edit services mobile-ip peer spi <i>hexadecimal-value</i>]
Release Information	Statement introduced in Junos OS Release 9.3. Support at the [edit logical-systems <i>logical-system-name</i> ...], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> ...], and [edit routing-instances <i>routing-instances-name</i> ...] hierarchy levels introduced in Junos OS Release 9.5.
Description	Configure the security parameter for the peer entity—, either a mobile node, home agent, or foreign agent.
Options	host —Use the mobile node in home agent mobility-agent —Use the home agent or foreign agent
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring Mobile IP on page 17 • Configuring the Mobile IP Home Agent on page 19

generic

Syntax	generic;
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> services mobile-ip access-type], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> services mobile-ip access-type], [edit routing-instances <i>routing-instance-name</i> services mobile-ip access-type], [edit services mobile-ip access-type]
Release Information	Statement introduced in Junos OS Release 9.5.
Description	Disable WiMAX features for Mobile IP home agent, preventing interoperability in a WiMAX environment.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring Mobile IP on page 17 • Configuring the Access Type for Mobile IP on page 22

home-agent (Mobile IP Networks)

Syntax	<pre>home-agent { enable-service <i>interface-name</i>; virtual-network { home-agent-address <i>ip-address</i> { registration-lifetime <i>seconds</i>; revocation-required; timestamp-tolerance <i>seconds</i>; } } }</pre>
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> services mobile-ip], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> services mobile-ip], [edit routing-instances <i>routing-instances-name</i> services mobile-ip], [edit services mobile-ip]
Release Information	Statement introduced in Junos OS Release 9.3. Support at the [edit logical-systems <i>logical-system-name</i> services mobile-ip], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> services mobile-ip], and [edit routing-instances <i>routing-instances-name</i> services mobile-ip] hierarchy levels introduced in Junos OS Release 9.5.
Description	Define the virtual networks and non-virtual networks for the Mobile IP home agent. The remaining statements are explained separately.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Mobile IP on page 17

home-agent (Mobile IP Dynamic Assignment)

Syntax	<pre>home-agent { nai (name@domain @domain) { home-agent ip-address; } }</pre>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> services mobile-ip dynamic-home-assignment], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> services mobile-ip dynamic-home-assignment], [edit routing-instances <i>routing-instances-name</i> services mobile-ip dynamic-home-assignment], [edit services mobile-ip dynamic-home-assignment]</p>
Release Information	<p>Statement introduced in Junos OS Release 9.3. Support at the [edit logical-systems <i>logical-system-name</i> services mobile-ip dynamic-home-assignment], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> services mobile-ip dynamic-home-assignment], and [edit routing-instances <i>routing-instances-name</i> services mobile-ip dynamic-home-assignment] hierarchy levels introduced in Junos OS Release 9.5.</p>
Description	<p>Configure the IP address to which registration requests are sent as part of the home agent's dynamic assignment rule.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>system—To view this statement in the configuration. system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Mobile IP on page 17 • Configuring Dynamic Home Assignment for the Mobile Node on page 21

home-agent (Mobile IP Network Address Identifier)

Syntax	<code>home-agent <i>ip-address</i>;</code>
Hierarchy Level	<code>[edit services mobile-ip dynamic-home-assignment home-agent <i>nai name@domain</i>],</code> <code>[edit logical-systems <i>logical-system-name</i> services mobile-ip dynamic-home-assignment</code> <code>home-agent <i>nai name@domain</i>],</code> <code>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> services</code> <code>mobile-ip dynamic-home-assignment home-agent <i>nai name@domain</i>],</code> <code>[edit routing-instances <i>routing-instance-name</i> services mobile-ip dynamic-home-assignment</code> <code>home-agent <i>nai name@domain</i>],</code> <code>[edit services mobile-ip dynamic-home-assignment home-agent <i>nai @domain</i>],</code> <code>[edit logical-systems <i>logical-system-name</i> services mobile-ip dynamic-home-assignment</code> <code>home-agent <i>nai @domain</i>],</code> <code>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> services</code> <code>mobile-ip dynamic-home-assignment home-agent <i>nai @domain</i>],</code> <code>[edit routing-instances <i>routing-instance-name</i> services mobile-ip dynamic-home-assignment</code> <code>home-agent <i>nai @domain</i>]</code>
Release Information	Statement introduced in Junos OS Release 9.3.
Description	Configure the IP address to which registration requests are sent as part of the home agent's dynamic assignment rule.
Options	<i>ip-address</i> —IP address of the home agent
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Mobile IP on page 17• Configuring Dynamic Home Assignment for the Mobile Node on page 21

home-agent-address

Syntax	<pre>home-agent-address <i>ip-address</i> { registration-lifetime <i>seconds</i>; revocation-required; timestamp-tolerance <i>seconds</i>; }</pre>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> services mobile-ip home-agent virtual-network], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> services mobile-ip home-agent virtual-network], [edit routing-instances <i>routing-instances-name</i> services mobile-ip home-agent virtual-network], [edit services mobile-ip home-agent virtual-network]</p>
Release Information	<p>Statement introduced in Junos OS Release 9.3. Support at the [edit logical-systems <i>logical-system-name</i> services mobile-ip home-agent virtual-network], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> services mobile-ip home-agent virtual-network], and [edit routing-instances <i>routing-instances-name</i> services mobile-ip home-agent virtual-network] hierarchy levels introduced in Junos OS Release 9.5.</p>
Description	<p>Defines addressing for the virtual network of the Mobile IP home agent.</p>
Options	<p><i>ip-address</i>—For virtual networks, the loopback IP address for the virtual network. For non-virtual networks, a public address.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>system—To view this statement in the configuration. system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Mobile IP on page 17 • Configuring the Mobile IP Home Agent on page 19

key

Syntax	<code>key (hex ascii) <i>string</i>;</code>
Hierarchy Level	<code>[edit logical-systems <i>logical-system-name</i> services mobile-ip peer ip-address <i>address</i> spi <i>hexadecimal-value</i>],</code> <code>[edit logical-systems <i>logical-system-name</i> services mobile-ip peer nai <i>name@domain</i> spi <i>hexadecimal-value</i>],</code> <code>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> services mobile-ip peer ip-address <i>address</i> spi <i>hexadecimal-value</i>],</code> <code>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> services mobile-ip peer nai <i>name@domain</i> spi <i>hexadecimal-value</i>],</code> <code>[edit routing-instances <i>routing-instances-name</i> services mobile-ip peer ip-address <i>address</i> spi <i>hexadecimal-value</i>],</code> <code>[edit routing-instances <i>routing-instances-name</i> services mobile-ip peer nai <i>name@domain</i> spi <i>hexadecimal-value</i>],</code> <code>[edit services mobile-ip peer ip-address <i>address</i> spi <i>hexadecimal-value</i>],</code> <code>[edit services mobile-ip peer nai <i>name@domain</i> spi <i>hexadecimal-value</i>]</code>
Release Information	Statement introduced in Junos OS Release 9.3. Support at the <code>[edit logical-systems <i>logical-system-name</i> ...]</code> , <code>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> ...]</code> , and <code>[edit routing-instances <i>routing-instances-name</i> ...]</code> hierarchy levels introduced in Junos OS Release 9.5.
Description	Configure the authentication key for the security association, in either HEX or ASCII format. The resulting 128-bit key is specified as a hexadecimal number with each character in the range 0x0–0xF.
Options	<code>hex <i>string</i></code> —Key specified in HEX format <code>ascii <i>string</i></code> —Key specified in ASCII format
Required Privilege Level	<code>system</code> —To view this statement in the configuration. <code>system-control</code> —To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Mobile IP on page 17• Configuring the Mobile IP Home Agent on page 19

mobile-ip

Syntax	<pre> mobile-ip { access-type { (generic wimax); } authenticate { order (aaa local); } dynamic-home-assignment { home-agent { nai (name@domain @domain) { home-agent ip-address; } } } home-agent { enable-service interface-name; virtual-network { home-agent-address ip-address { registration-lifetime seconds; revocation-required; timestamp-tolerance seconds; } } } peer { (ip-address address nai name@domain) { spi hexadecimal-value { algorithm (hmac-md5 md5); entity-type (host mobility-agent); key (hex ascii) string; replay-method (none timestamp seconds); } } } traceoptions { file filename <files number> <match regular-expression > <size maximum-file-size> <world-readable no-world-readable>; flag flag; level (all error info notice verbose warning); no-remote-trace; } } </pre>
Hierarchy Level	<p>[edit services], [edit logical-systems <i>logical-system-name</i> services], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> services], [edit routing-instances <i>routing-instances-name</i> services]</p>
Release Information	<p>Statement introduced in Junos OS Release 9.3. Support at the [edit logical-systems <i>logical-system-name</i> services], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> services], and [edit</p>

routing-instances *routing-instances-name* services] hierarchy levels introduced in Junos OS Release 9.5.


Description Configure Junos Mobile IP features.

The remaining statements are explained separately.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation • [Configuring the Mobile IP Home Agent on page 19](#)

nai

Syntax	<code>nai (name@domain @domain) { home-agent ip-address; }</code>
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> services mobile-ip dynamic-home-assignment home-agent], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> services mobile-ip dynamic-home-assignment home-agent], [edit routing-instances <i>routing-instances-name</i> services mobile-ip dynamic-home-assignment home-agent], [edit services mobile-ip dynamic-home-assignment home-agent]
Release Information	Statement introduced in Junos OS Release 9.3. Support at the [edit logical-systems <i>logical-system-name</i> ...], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> ...], and [edit routing-instances <i>routing-instances-name</i> ...] hierarchy levels introduced in Junos OS Release 9.5.
Description	Configure the network address identifiers (NAI) to which registration requests are sent as part of the home agent's dynamic assignment rule .
Options	<i>name@domain</i> —User at a specified domain <i>@domain</i> —All users at a specified domain
<div>  <p>NOTE: The <i>name</i> can include only alphanumeric characters, dots, hyphens, or underscores. The <i>name</i> cannot end in @; @ must be used to separate <i>name</i> and <i>domain</i>. The <i>domain</i> can include only alphanumeric characters, dots, or hyphens. The <i>domain</i> must be in the format <i>domain.suffix</i>, where the <i>suffix</i> is com, org, net, and so on. The <i>suffix</i> must consist of at least two alphanumeric characters.</p> </div>	
The remaining statement is explained separately.	
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring Mobile IP on page 17 • Configuring Dynamic Home Assignment for the Mobile Node on page 21

order (Mobile IP)

Syntax	<code>order (aaa local);</code>
Hierarchy Level	<code>[edit logical-systems <i>logical-system-name</i> services mobile-ip authenticate]</code> , <code>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> services mobile-ip authenticate]</code> , <code>[edit routing-instances <i>routing-instances-name</i> services mobile-ip authenticate]</code> , <code>[edit services mobile-ip authenticate]</code>
Release Information	Statement introduced in Junos OS Release 9.3. Support at the <code>[edit logical-systems <i>logical-system-name</i> ...]</code> , <code>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> ...]</code> , and <code>[edit routing-instances <i>routing-instances-name</i> ...]</code> hierarchy levels introduced in Junos OS Release 9.5.
Description	Define the authentication method performed for Mobile IP.
Default	AAA is the default authentication method.
Options	aaa —Authentication is performed by AAA. This option is available only in the default router and default routing instance, and therefore only in the <code>[edit services mobile-ip]</code> hierarchy level. local —Authentication is performed using parameters defined in the local database.
Required Privilege Level	system —To view this statement in the configuration. system-control —To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Mobile IP on page 17• Configuring the Access Type for Mobile IP on page 22

peer

Syntax	<pre>peer { (ip-address <i>address</i> nai <i>name@domain</i>) { spi <i>hexadecimal-value</i> { algorithm (hmac-md5 md5); entity-type (host mobility-agent); key (hex ascii) <i>string</i>; replay-method (timestamp <i>seconds</i> none); } } }</pre>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> services mobile-ip], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> services mobile-ip], [edit routing-instances <i>routing-instances-name</i> services mobile-ip], [edit services mobile-ip]</p>
Release Information	<p>Statement introduced in Junos OS Release 9.3.</p> <p>Support at the [edit logical-systems <i>logical-system-name</i> ...], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> ...], and [edit routing-instances <i>routing-instances-name</i> ...] hierarchy levels introduced in Junos OS Release 9.5.</p>
Description	<p>Define the authentication configurations for a home agent mobile node. An authentication enables the registration message as acceptable to the final recipient of the registration message.</p>
Options	<p>ip-address <i>address</i>—IP address of the peer.</p> <p>nai <i>name@domain</i>—Network address identifier (NAI) of the peer. The <i>name</i> can include only alphanumeric characters, dots, hyphens, or underscores. The <i>name</i> cannot end in @; @ must be used to separate <i>name</i> and <i>domain</i>. The <i>domain</i> can include only alphanumeric characters, dots, or hyphens. The <i>domain</i> must be in the format <i>domain.suffix</i>, where the <i>suffix</i> is com, org, net, and so on. The <i>suffix</i> must consist of at least two alphanumeric characters.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Mobile IP on page 17 • Configuring the Mobile IP Home Agent on page 19

registration-lifetime

Syntax	<code>registration-lifetime seconds;</code>
Hierarchy Level	<code>[edit logical-systems <i>logical-system-name</i> services mobile-ip home-agent virtual-network home-agent-address ip-address],</code> <code>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> services mobile-ip home-agent virtual-network home-agent-address ip-address],</code> <code>[edit routing-instances <i>routing-instances-name</i> services mobile-ip home-agent virtual-network home-agent-address ip-address],</code> <code>[edit services mobile-ip home-agent virtual-network home-agent-address ip-address]</code>
Release Information	Statement introduced in Junos OS Release 9.3. Support at the <code>[edit logical-systems <i>logical-system-name</i> ...]</code> , <code>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> ...]</code> , and <code>[edit routing-instances <i>routing-instances-name</i> ...]</code> hierarchy levels introduced in Junos OS Release 9.5.
Description	Configure maximum period for registration lifetime that is accepted by the Mobile IP home agent.
Options	registration-lifetime seconds —Maximum lifetime that the home agent accepts in any registration request. The registration lifetime is not affected if you change the system clock. Range: 7 through 65535 seconds Default: 3600 seconds
Required Privilege Level	<code>system</code> —To view this statement in the configuration. <code>system-control</code> —To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Mobile IP on page 17• Configuring the Mobile IP Home Agent on page 19

replay-method

Syntax	<code>replay-method (none timestamp <i>seconds</i>);</code>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> services mobile-ip peer ip-address <i>address</i> spi <i>hexadecimal-value</i>].</p> <p>[edit logical-systems <i>logical-system-name</i> services mobile-ip peer <i>nai@domain</i> spi <i>hexadecimal-value</i>].</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> services mobile-ip peer ip-address <i>address</i> spi <i>hexadecimal-value</i>].</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> services mobile-ip peer <i>nai@domain</i> spi <i>hexadecimal-value</i>].</p> <p>[edit routing-instances <i>routing-instances-name</i> services mobile-ip peer ip-address <i>address</i> spi <i>hexadecimal-value</i>].</p> <p>[edit routing-instances <i>routing-instances-name</i> services mobile-ip peer <i>nai@domain</i> spi <i>hexadecimal-value</i>],</p> <p>[edit services mobile-ip peer ip-address <i>address</i> spi <i>hexadecimal-value</i>],</p> <p>[edit services mobile-ip peer <i>nai@domain</i> spi <i>hexadecimal-value</i>]</p>
Release Information	<p>Statement introduced in Junos OS Release 9.3.</p> <p>Support at the [edit logical-systems <i>logical-system-name</i> ...], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> ...], and [edit routing-instances <i>routing-instances-name</i> ...] hierarchy levels introduced in Junos OS Release 9.5.</p>
Description	Configure the replay protection method. The Identification field enables the home agent to verify that a registration message has been recently generated by the mobile node, rather than replayed by an attacker from a previous registration. You can specify a timestamp tolerance for the mobile node, which causes the request to be rejected if the tolerance is exceeded, or you can specify that the tolerance be taken from the value configured on the home agent.
Default	If you do not configure the replay protection method, then the timestamp tolerance is taken from the home agent by default.
Options	<p>none—Timestamp tolerance is obtained from the setting configured for the home agent</p> <p>timestamp <i>seconds</i>—Tolerance time in which a registration request timestamp and the local time of the home agent can differ.</p> <p>Range: 1 through 255 seconds</p>
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Mobile IP on page 17 • Configuring the Mobile IP Home Agent on page 19

revocation-required

Syntax	revocation-required;
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> services mobile-ip home-agent virtual-network home-agent-address ip-address], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> services mobile-ip home-agent virtual-network home-agent-address ip-address], [edit routing-instances <i>routing-instances-name</i> services mobile-ip home-agent virtual-network home-agent-address ip-address], [edit services mobile-ip home-agent virtual-network home-agent-address ip-address]
Release Information	Statement introduced in Junos OS Release 9.3. Support at the [edit logical-systems <i>logical-system-name</i> ...], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> ...], and [edit routing-instances <i>routing-instances-name</i> ...] hierarchy levels introduced in Junos OS Release 9.5.
Description	Configure the Mobile IP home agent to accept registration revocation requests only when the request includes the revocation extension.
Default	The Mobile IP home agent supports registration revocation requests that include the revocation extension, but it does not require the extension.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Mobile IP on page 17• Configuring the Mobile IP Home Agent on page 19

spi

Syntax	<pre>spi <i>hexadecimal-value</i> { algorithm (hmac-md5 md5); entity-type (host mobility-agent); key (hex ascii) <i>string</i>; replay-method (none timestamp <i>seconds</i>); }</pre>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> services mobile-ip peer ip-address <i>address</i>], [edit logical-systems <i>logical-system-name</i> services mobile-ip peer nai <i>user@domain</i>], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> services mobile-ip peer ip-address <i>address</i>], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> services mobile-ip peer nai <i>user@domain</i>], [edit routing-instances <i>routing-instances-name</i> services mobile-ip peer ip-address <i>address</i>], [edit routing-instances <i>routing-instances-name</i> services mobile-ip peer nai <i>user@domain</i>], [edit services mobile-ip peer ip-address <i>address</i>], [edit services mobile-ip peer nai <i>user@domain</i>]</p>
Release Information	<p>Statement introduced in Junos OS Release 9.3.</p> <p>Support at the [edit logical-systems <i>logical-system-name</i> services mobile-ip peer ip-address <i>address</i>], [edit logical-systems <i>logical-system-name</i> services mobile-ip peer nai <i>user@domain</i>], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> services mobile-ip peer ip-address <i>address</i>], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> services mobile-ip peer nai <i>user@domain</i>], [edit routing-instances <i>routing-instances-name</i> services mobile-ip peer ip-address <i>address</i>], and [edit routing-instances <i>routing-instances-name</i> services mobile-ip peer nai <i>user@domain</i>] hierarchy levels introduced in Junos OS Release 9.5.</p>
Description	<p>Define the security parameter index for identifying a security context between a pair of nodes among the contexts available in the Mobility Security Association. The index selects the authentication algorithm and key.</p>
Options	<p><i>hexadecimal-value</i>—Security parameter index identifier.</p> <p>Range: 100 to FFFFFFFF</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Mobile IP on page 17 • Configuring the Mobile IP Home Agent on page 19

statistics (Access Profile)

Syntax	statistics (time volume-time);
Hierarchy Level	[edit access profile <i>profile-name</i> accounting]
Release Information	Statement introduced in Junos OS Release 9.1. Statement introduced in Junos OS Release 9.1 for EX Series switches. Option volume-time introduced in Junos OS Release 9.4.
Description	Configure the router or switch to collect time statistics, or both volume and time statistics, for the sessions being managed by AAA.
Options	time —Collect uptime statistics only. volume-time —Collect both volume and uptime statistics. This option is not available for Mobile IP.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Mobile IP Home Agent Elements and Behavior on page 3• <i>Configuring Authentication and Accounting Parameters for Subscriber Access</i>

timestamp-tolerance

Syntax	<code>timestamp-tolerance <i>seconds</i>;</code>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> services mobile-ip home-agent virtual-network home-agent-address <i>ip-address</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> services mobile-ip home-agent virtual-network home-agent-address <i>ip-address</i>],</p> <p>[edit routing-instances <i>routing-instances-name</i> services mobile-ip home-agent virtual-network home-agent-address <i>ip-address</i>],</p> <p>[edit services mobile-ip home-agent virtual-network home-agent-address <i>ip-address</i>]</p>
Release Information	<p>Statement introduced in Junos OS Release 9.3.</p> <p>Support at the [edit logical-systems <i>logical-system-name</i> ...], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> ...], and [edit routing-instances <i>routing-instances-name</i> ...] hierarchy levels introduced in Junos OS Release 9.5.</p>
Description	Configure the acceptable difference between a registration request timestamp and the local time of the home agent.
Options	<p>timestamp-tolerance <i>seconds</i>—Acceptable difference in time between a registration request timestamp and the local time of the home agent.</p> <p>Range: 1 through 255 seconds</p> <p>Default: 7 seconds</p>
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Mobile IP on page 17 • Configuring the Mobile IP Home Agent on page 19

traceoptions (Mobile IP)

Syntax	<pre>traceoptions { file <i>filename</i> <files <i>number</i>> <match <i>regular-expression</i> > <size <i>maximum-file-size</i>> <world-readable no-world-readable>; flag <i>flag</i>; level (all error info notice verbose warning); no-remote-trace; }</pre>
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> services mobile-ip], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> services mobile-ip], [edit routing-instances <i>routing-instances-name</i> services mobile-ip], [edit services mobile-ip]
Release Information	Statement introduced in Junos OS Release 9.3. Support at the [edit logical-systems <i>logical-system-name</i> ...], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> ...], and [edit routing-instances <i>routing-instances-name</i> ...] hierarchy levels introduced in Junos OS Release 9.5.
Description	Define tracing operations for Mobile IP processes.
Options	file <i>filename</i> — Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory /var/log . Ensure that filenames are unique for each logical system or routing instance in which Mobile IP is configured.



NOTE: Global messages (common to all logical systems and routing instances) are always saved in **/var/log/mipd**. Messages that are specific to a logical system or routing instance are never saved in **/var/log/mipd**. If you do not configure a trace filename for a logical system or routing instance, then nothing is traced for that entity.

files *number*—(Optional) Maximum number of trace files to create before overwriting the oldest one. If you specify a maximum number of files, you also must specify a maximum file size with the **size** option.

Range: 2 through 1000

Default: 3 files

flag *flag*—Tracing operation to perform. To specify more than one tracing operation, include multiple **flag** statements. You can include the following flags:

- **all**—Trace all operations.
- **authentication**—Trace authentication operations.
- **binding**—Trace bindings.

- **event**—Trace events.
- **ha-fsm**—Trace home agent state machine operations.
- **home-agent**—Trace home agent operations.
- **interface-database**—Trace interface database operations.
- **packet**—Trace packet decoding operations.
- **protocol**—Trace protocol operations.
- **rtsock**—Trace routing socket operations.
- **session-db**—Trace session database events.
- **signal**—Trace signal operations.
- **subscriber**—Trace subscriber events.
- **timer**—Trace timer events.
- **trace**—Trace changes in tracing.
- **tunnel**—Trace tunneling operations.
- **user-interface**—Trace user interface events.

level—Specify level of tracing to perform. You can specify any of the following levels:

- **all**—Match all levels.
- **error**—Match error conditions.
- **info**—Match informational messages.
- **notice**—Match notice messages about conditions requiring special handling.
- **verbose**—Match verbose messages.
- **warning**—Match warning messages.

match *regular-expression*—(Optional) Refine the output to include lines that contain the regular expression.

no-remote-trace—Disable remote tracing.

no-world-readable—(Optional) Disable unrestricted file access.

size *maximum-file-size*—(Optional) Maximum size of each trace file. By default, the number entered is treated as bytes. Alternatively, you can include a suffix to the number to indicate kilobytes (KB), megabytes (MB), or gigabytes (GB). If you specify a maximum file size, you also must specify a maximum number of trace files with the **files** option.

Syntax: **size***k* to specify KB, **size***m* to specify MB, or **size***g* to specify GB

Range: 10240 through 1073741824

Default: 128 KB

world-readable—(Optional) Enable unrestricted file access.

Required Privilege Level trace—To view this statement in the configuration.
trace-control—To add this statement to the configuration.

Related Documentation

- [Tracing Mobile IP Operations for Subscriber Access on page 69](#)

wimax

Syntax wimax;

Hierarchy Level [edit services [mobile-ip](#) access-type],
[edit logical-systems *logical-system-name* services [mobile-ip](#) access-type],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* services [mobile-ip](#) access-type],
[edit routing-instances *routing-instance-name* services [mobile-ip](#) access-type]

Release Information Statement introduced in Junos OS Release 9.5.

Description Enable WiMAX features for Mobile IP home agent, including the ability to process, send, and receive WiMAX Vendor Specific Attributes (VSAs).



.....
NOTE: Although this statement is available in the CLI for both default and nondefault router contexts, the commit operation is disallowed when you configure the statement in a nondefault router context.
.....

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- [Configuring Mobile IP on page 17](#)
- [Configuring the Access Type for Mobile IP on page 22](#)

virtual-network

Syntax	<pre>virtual-network { home-agent-address ip-address { registration-lifetime seconds; revocation-required; timestamp-tolerance seconds; } }</pre>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> services mobile-ip home-agent], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> services mobile-ip home-agent], [edit routing-instances <i>routing-instances-name</i> services mobile-ip home-agent], [edit services mobile-ip home-agent]</p>
Release Information	<p>Statement introduced in Junos OS Release 9.3.</p> <p>Support at the [edit logical-systems <i>logical-system-name</i> ...], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> ...], and [edit routing-instances <i>routing-instances-name</i> ...] hierarchy levels introduced in Junos OS Release 9.5.</p>
Description	<p>Define the virtual network for the Mobile IP home agent. Only one virtual network is supported.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Mobile IP on page 17 • Configuring the Mobile IP Home Agent on page 19

PART 3

Administration

- [Monitoring Commands on page 53](#)

CHAPTER 5

Monitoring Commands

clear mobile-ip binding

Syntax	<code>clear mobile-ip binding</code> (<code>all</code> <code>ip-address</code> <i>ip-address</i> <code>nai</code> <i>nai-string</i>) < <code>logical-system</code> <i>logical-system-name</i> > < <code>routing-instance</code> <i>routing-instance-name</i> >
Release Information	Command introduced in Junos OS Release 9.3.
Description	Clear the Mobile IP binding.
Options	<p>all—Clear all Mobile IP bindings.</p> <p>ip-address <i>ip-address</i>—Clear the Mobile IP bindings for the specified IP home address (HoA).</p> <p>nai <i>nai-string</i>—Clear the Mobile IP bindings for the specified network access identifier.</p> <p>logical-system <i>logical-system-name</i>—(Optional) Clear the Mobile IP bindings for the specified logical system.</p> <p>routing-instance <i>routing-instance-name</i>—(Optional) Clear the Mobile IP bindings for the specified routing instance.</p>
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none">• show mobile-ip home-agent bindings on page 57
List of Sample Output	clear mobile-ip binding on page 54
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear mobile-ip binding

```
user@host> clear mobile-ip binding all
```

show mobile-ip home-agent overview

Syntax	show mobile-ip home-agent overview <logical-system <i>logical-system-name</i> > <routing-instance <i>routing-instance-name</i> >
Release Information	Command introduced in Junos OS Release 9.3.
Description	Display overview information for Mobile IP home agent.
Options	<p>logical-system <i>logical-system-name</i>—(Optional) Display information for the specified logical system.</p> <p>routing-instance <i>routing-instance-name</i>—(Optional) Display information for the specified routing instance.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • show mobile-ip home-agent bindings on page 57 • show mobile-ip home-agent traffic on page 60 • show mobile-ip home-agent virtual-network on page 63 • show mobile-ip wimax release on page 65
List of Sample Output	show mobile-ip home-agent overview on page 55
Output Fields	Table 5 on page 55 lists the output fields for the show mobile-ip home-agent overview command. Output fields are listed in the approximate order in which they appear.

Table 5: show mobile-ip home-agent overview Output Fields

Field Name	Field Description
Status	Total number of registration requests received.
Service Enabled on	Total number of registration requests forwarded.
Home Agents	Total number of registration requests denied.
Authentication	Total number of registration replies sent.

Sample Output

show mobile-ip home-agent overview

```

user@host> show mobile-ip home-agent overview
Status                : Active
Service Enabled on    : ge-0/0/3.0, ge-0/0/2.0
Home agents           : 10.1.1.1, 20.1.1.1, 55.55.55.1
Authentication        : AAA

```


show mobile-ip home-agent bindings

Syntax	show mobile-ip home-agent bindings <ip-address <i>ip-address</i> nai <i>nai-string</i> summary> <logical-system <i>logical-system-name</i> > <routing-instance <i>routing-instance-name</i> >
Release Information	Command introduced in Junos OS Release 9.3.
Description	Display information about Mobile IP home agent bindings.
Options	<p>ip-address <i>ip-address</i>—(Optional) Display information for the specified Mobile IP home address.</p> <p>logical-system <i>logical-system-name</i>—(Optional) Display information for the specified logical system.</p> <p>nai <i>nai-string</i>—(Optional) Display information for the specified Mobile IP network access identifier.</p> <p>routing-instance <i>routing-instance-name</i>—(Optional) Display information for the specified routing instance.</p> <p>summary—(Optional) Display only summary (total bindings) information.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • clear mobile-ip binding on page 54 • show mobile-ip home-agent overview on page 55 • show mobile-ip home-agent traffic on page 60 • show mobile-ip home-agent virtual-network on page 63 • show mobile-ip wimax release on page 65
List of Sample Output	show mobile-ip home-agent bindings on page 58 show mobile-ip home-agent bindings ip-address on page 58 show mobile-ip home-agent bindings nai on page 59 show mobile-ip home-agent bindings summary on page 59
Output Fields	Table 6 on page 57 lists the output fields for the show mobile-ip home-agent bindings command. Output fields are listed in the approximate order in which they appear.

Table 6: show mobile-ip home-agent bindings Output Fields

Field Name	Field Description
Home Address	Home address of the mobile node.
NAI	Network access identifier of the mobile node.

Table 6: show mobile-ip home-agent bindings Output Fields (*continued*)

Field Name	Field Description
Home agent	Home agent address of the mobile node.
Care-of-address	Care of address used by the mobile node.
Lifetime Granted	Lifetime granted for the mobile node.
Lifetime Remaining	Remaining lifetime for the mobile node.
Tunnel Type	Type of tunnel requested by the mobile node.
Tunnel ID	Tunnel ID the mobile node is using.
Tunnel Source	Tunnel source address the mobile node is using.
Tunnel Destination	Tunnel destination address the mobile node is using.
Identification	Identification value received from the mobile node.
Revocation Support	Whether registration revocation is supported for this binding.
Notify MN	Whether mobile node notification has been negotiated.
Total Bindings	Total number of Mobile IP home agent bindings.

Sample Output

show mobile-ip home-agent bindings

```

user@host> show mobile-ip home-agent bindings
Home address  NAI           Home agent  Care-of-address
10.1.1.3      abcde@def.com  10.1.1.1   50.50.50.1
30.1.1.3      -              55.55.55.1 50.50.50.1
20.1.1.3      def@def.com    20.1.1.1   60.50.50.1

```

show mobile-ip home-agent bindings ip-address

```

user@host> show mobile-ip home-agent bindings ip-address 10.1.1.3
Home address      : 10.1.1.3
NAI               : abcde@def.com
Home agent        : 10.1.1.1
Care-of-address   : 50.50.50.1
Lifetime Granted  : 180
Lifetime Remaining : 20
Tunnel Type       : IP-IP
Tunnel ID         : 10
Tunnel Source     : 10.1.1.1
Tunnel Destination : 50.50.50.1
Identification    : ABCD1234.4321ABCD
Revocation Support : Enabled
Notify MN of Revocation : Enabled

```

show mobile-ip home-agent bindings nai

```
user@host> show mobile-ip home-agent bindings nai abcde@def.com
Home address      : 10.1.1.3
NAI               : abcde@def.com
Home agent        : 10.1.1.1
Care-of-address   : 50.50.50.1
Lifetime Granted  : 180
Lifetime Remaining : 20
Tunnel Type       : IP-IP
Tunnel ID         : 10
Tunnel Source     : 10.1.1.1
Tunnel Destination : 50.50.50.1
Identification    : ABCD1234.4321ABCD
Revocation Support : Enabled
Notify MN         : Enabled
```

show mobile-ip home-agent bindings summary

```
user@host> show mobile-ip home-agent bindings summary
Total bindings : 3
```

show mobile-ip home-agent traffic

Syntax	<code>show mobile-ip home-agent traffic</code> <code><logical-system <i>logical-system-name</i>></code> <code><routing-instance <i>routing-instance-name</i>></code>
Release Information	Command introduced in Junos OS Release 9.3.
Description	Display information about Mobile IP home agent protocol statistics.
Options	logical-system <i>logical-system-name</i> —(Optional) Display information for the specified logical system. routing-instance <i>routing-instance-name</i> —(Optional) Display information for the specified routing instance.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none">• show mobile-ip home-agent bindings on page 57• show mobile-ip home-agent overview on page 55• show mobile-ip home-agent virtual-network on page 63• show mobile-ip wimax release on page 65
List of Sample Output	show mobile-ip home-agent traffic on page 61
Output Fields	Table 7 on page 60 lists the output fields for the show mobile-ip home-agent traffic command. Output fields are listed in the approximate order in which they appear.

Table 7: show mobile-ip home-agent traffic Output Fields

Field Name	Field Description
Registration request received	Total number of registration requests received.
Registration request forwarded	Total number of registration requests forwarded.
Registration request denied	Total number of registration requests denied.
Registration replies sent	Total number of registration replies sent.
Registration Errors unspecified	Total number of registration requests denied by the home agent for reasons unspecified.

Table 7: show mobile-ip home-agent traffic Output Fields (*continued*)

Field Name	Field Description
Registration Errors Administrative prohibited	Total number of registration requests denied by home agent as “administrative prohibited.”
Registration Errors Insufficient Resource	Total number of registration requests denied by the home agent for insufficient resources.
Registration Errors Bad request form	Total number of registration requests denied by the home agent due to a bad request form.
Registration Errors Too many Bindings	Total number of registration requests denied by the home agent for having too many bindings.
Registration Errors Unknown HA	Total number of registration requests denied by the home agent for having an unknown home agent.
Registration Errors ID mismatch	Total number of registration requests denied by the home agent for having a mismatched ID.
Registration Errors Authentication failed MN	Total number of registration requests denied by the home agent because the mobile node failed authentication.
Registration Errors Authentication failed FA	Total number of registration requests denied by the home agent because the foreign agent failed authentication.

Sample Output

show mobile-ip home-agent traffic

```

user@host> show mobile-ip home-agent traffic
Registration Request
  Received   : 10
  Forwarded  : 5
  Denied     : 5
Registration Replies
  Sent       : 5
Registration Errors
  Unspecified      : 0
  Administrative prohibited : 0
  Insufficient Resource : 0
  Bad request form   : 0
  Too many Bindings  : 0
  Unknown HA         : 0
  ID mismatch        : 0
  Unavailable Reverse tunnel : 0
  Unavailable Encapsulation : 0
  Reverse Tunnel Mandatory : 0
  Authentication failed MN : 0
  Authentication failed FA : 0

```


show mobile-ip home-agent virtual-network

Syntax	show mobile-ip home-agent virtual-network <logical-system <i>logical-system-name</i> > <routing-instance <i>routing-instance-name</i> >
Release Information	Command introduced in Junos OS Release 9.3.
Description	Display information about Mobile IP home agent virtual networks.
Options	<p>logical-system <i>logical-system-name</i>—(Optional) Display information for the specified logical system.</p> <p>routing-instance <i>routing-instance-name</i>—(Optional) Display information for the specified routing instance.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • show mobile-ip home-agent bindings on page 57 • show mobile-ip home-agent overview on page 55 • show mobile-ip home-agent traffic on page 60 • show mobile-ip wimax release on page 65
List of Sample Output	show mobile-ip home-agent virtual-network on page 64
Output Fields	Table 8 on page 63 lists the output fields for the show mobile-ip home-agent virtual-network command. Output fields are listed in the approximate order in which they appear.

Table 8: show mobile-ip home-agent virtual-network Output Fields

Field Name	Field Description
Home agent address	Home agent address of the mobile node.
Registration Lifetime	Maximum registration lifetime that home agent allows.
Time Tolerance	Number of seconds the time stamp may differ.
Address Pool	Address pool configured.
Total MNs	Current number of mobile nodes that the home agent is serving.
Home address	Home address of the mobile node.
NAI	Network access identifier of the mobile node.

Table 8: show mobile-ip home-agent virtual-network Output Fields (*continued*)

Field Name	Field Description
Care-of-address	Care of address used by the mobile node.
RegLifetime Granted	Lifetime granted for the mobile node.
RegLifetime Remaining	Remaining lifetime for the mobile node.

Sample Output

show mobile-ip home-agent virtual-network

```
user@host> show mobile-ip home-agent virtual-network
Home Agent Address      : 55.55.55.55
Registration Lifetime    : 1800
Time Tolerance          : 120
Address Pool            : 10.1.1.10 - 10.1.1.50
Total MN's              : 2

MN's :
Home address            : 60.60.60.1
NAI                     : abcde@def.com
Care-of-address         : 50.50.50.1
Reglifetime granted     : 120
Reglifetime remaining: 100

Home address            : 70.70.70.1
NAI                     : def@def.com
Care-of-address         : 80.80.80.1
Reglifetime granted     : 120
Reglifetime remaining: 100
```


show mobile-ip wimax release

Syntax	show mobile-ip wimax release <logical-system <i>logical-system-name</i> > <routing-instance <i>routing-instance-name</i> >
Release Information	Command introduced in Junos OS Release 9.5.
Description	Display the WiMAX Forum Network Architecture release that is supported by the current Mobile IP implementation.
Options	<p>logical-system <i>logical-system-name</i>—(Optional) Display information for the specified logical system.</p> <p>routing-instance <i>routing-instance-name</i>—(Optional) Display information for the specified routing instance.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • show mobile-ip home-agent bindings on page 57 • show mobile-ip home-agent overview on page 55 • show mobile-ip home-agent traffic on page 60 • show mobile-ip home-agent virtual-network on page 63
List of Sample Output	show mobile-ip wimax release on page 65
Output Fields	Table 9 on page 65 lists the output fields for the show mobile-ip wimax release command. Output fields are listed in the approximate order in which they appear.

Table 9: show mobile-ip wimax release Output Fields

Field Name	Field Description
Release	WiMAX Forum Network Architecture release number.
Version	WiMAX Forum Network Architecture version number.

Sample Output

show mobile-ip wimax release

```
user@host> show mobile-ip wimax release
Release 1, Version 1.2
```


PART 4

Troubleshooting

- [Acquiring Troubleshooting Information on page 69](#)
- [Troubleshooting Configuration Statement on page 77](#)

CHAPTER 6

Acquiring Troubleshooting Information

- [Tracing Mobile IP Operations for Subscriber Access on page 69](#)
- [Configuring the Mobile IP Trace Log Filename on page 71](#)
- [Configuring the Number and Size of Mobile IP Log Files on page 71](#)
- [Configuring Access to the Mobile IP Log File on page 72](#)
- [Configuring a Regular Expression for Mobile IP Messages to Be Logged on page 72](#)
- [Configuring the Mobile IP Tracing Flags on page 72](#)
- [Configuring the Severity Level to Filter Which Mobile IP Messages Are Logged on page 73](#)
- [Collecting Subscriber Access Logs Before Contacting Juniper Technical Support on page 73](#)

Tracing Mobile IP Operations for Subscriber Access

The Junos OS trace feature tracks Mobile IP operations and records events in a log file. The error descriptions captured in the log file provide detailed information to help you solve problems.

Trace-related configurations are independent for each logical system and routing instance in which Mobile IP is configured. Mobile IP can generate two types of log messages:

- Trace messages common to all logical systems and routing instances in which Mobile IP is configured. Examples of this global message type are the messages generated by Mobile IP during initialization after it starts up. These trace messages are stored in the default trace file, **/var/log/mipd**. You cannot configure Mobile IP to save global messages in a different file. Mobile IP traces global messages by default.
- Trace messages specific to a logical system or routing instance in which Mobile IP is configured. An example of this message type is the message generated by Mobile IP when it receives a registration request. These trace messages are stored in the trace file configured for that logical system or routing instance. These messages cannot be saved in **/var/log/mipd**.

By default, nothing is traced. When you enable the tracing operation, the default tracing behavior is as follows:

1. Important events are logged in a file located in the **/var/log** directory. By default, the router uses the filename **mipd** for global tracing. You can specify a different filename,

but you cannot change the directory in which trace files are located. Logical system and routing instance messages are logged in a file that you must configure separately from **mipd** in the **/var/log** directory.

2. When the trace log file **filename** reaches 128 kilobytes (KB), it is compressed and renamed **filename.0.gz**. Subsequent events are logged in a new file called **filename**, until it reaches capacity again. At this point, **filename.0.gz** is renamed **filename.1.gz** and **filename** is compressed and renamed **filename.0.gz**. This process repeats until the number of archived files reaches the maximum file number. Then the oldest trace file—the one with the highest number—is overwritten.

You can optionally specify the number of trace files to be from 2 through 1000. You can also configure the maximum file size to be from 10 KB through 1 gigabyte (GB). (For more information about how log files are created, see the *Junos OS System Log Messages Reference*.)

By default, only the user who configures the tracing operation can access log files. You can optionally configure read-only access for all users.

To configure Mobile IP tracing operations:

1. (Optional) Configure a trace log filename.
See [“Configuring the Mobile IP Trace Log Filename” on page 71](#).
2. (Optional) Configure the number and size of trace logs.
See [“Configuring the Number and Size of Mobile IP Log Files” on page 71](#).
3. (Optional) Configure user access to trace logs.
See [“Configuring Access to the Mobile IP Log File” on page 72](#).
4. (Optional) Configure a regular expression to filter the information to be included in the trace log.
See [“Configuring a Regular Expression for Mobile IP Messages to Be Logged” on page 72](#).
5. (Optional) Configure flags to specify which events are logged.
See [“Configuring the Mobile IP Tracing Flags” on page 72](#).
6. (Optional) Configure a severity level for messages to specify which event messages are logged.
See [“Configuring the Severity Level to Filter Which Mobile IP Messages Are Logged” on page 73](#).

Configuring the Mobile IP Trace Log Filename

Global messages common to all Mobile IP logical systems and routing instances are recorded only in `/var/log/mipd`. Mobile IP automatically creates this file if it is not present when Mobile IP starts. You cannot configure global messages to be recorded in any other file.

You must specify a different name with the `file` option for messages that are specific to a logical system or routing instance in which Mobile IP is configured. Ensure that filenames are unique for each logical system or routing instance in which Mobile IP is configured. If you do not configure a trace filename for a logical system or routing instance, then nothing is traced for that entity.

To configure the filename for Mobile IP tracing operations for a logical system or routing instance:

- Specify the name of the file used for the trace output.

```
[edit logical-systems lr1 services mobile-ip traceoptions]
user@host# set file mip-lr1_1
```

Related Documentation

- Tracing Mobile IP Operations for Subscriber Access on page 69

Configuring the Number and Size of Mobile IP Log Files

You can optionally specify the number of compressed, archived trace log files to be from 2 through 1000. You can also configure the maximum file size to be from 10 KB through 1 gigabyte (GB); the default size is 128 kilobytes (KB).

The archived files are differentiated by a suffix in the format `.number.gz`. The newest archived file is `.0.gz` and the oldest archived file is `.(maximum number)-1.gz`. When the current trace log file reaches the maximum size, it is compressed and renamed, and any existing archived files are renamed. This process repeats until the maximum number of archived files is reached, at which point the oldest file is overwritten.

For example, you can set the maximum file size to 2 MB, and the maximum number of files to 20. When the file that receives the output of the tracing operation, `filename`, reaches 2 MB, `filename` is compressed and renamed `filename.0.gz`, and a new file called `filename` is created. When the new `filename` reaches 2 MB, `filename.0.gz` is renamed `filename.1.gz` and `filename` is compressed and renamed `filename.0.gz`. This process repeats until there are 20 trace files. Then the oldest file, `filename.19.gz`, is simply overwritten when the next oldest file, `filename.18.gz` is compressed and renamed to `filename.19.gz`.

To configure the number and size of trace files:

- Specify the name, number, and size of the file used for the trace output. (Mobile IP supports the `files` and `size` options for the `traceoptions` statement.)

```
[edit services mobile-ip traceoptions]
user@host# set file mip_1 _logfile_1 files 20 size 2097152
```

- Related Documentation**
- [Tracing Mobile IP Operations for Subscriber Access on page 69](#)

Configuring Access to the Mobile IP Log File

By default, only the user who configures the tracing operation can access the log files. You can enable all users to read the log file and you can explicitly set the default behavior of the log file.

To specify that all users can read the log file:

- Configure the log file to be world-readable.

```
[edit services mobile-ip traceoptions]  
user@host# set file mip_1_logfile_1 world-readable
```

To explicitly set the default behavior, only the user who configured tracing can read the log file:

- Configure the log file to be no-world-readable.

```
[edit services mobile-ip traceoptions]  
user@host# set file mip_1_logfile_1 no-world-readable
```

- Related Documentation**
- [Tracing Mobile IP Operations for Subscriber Access on page 69](#)

Configuring a Regular Expression for Mobile IP Messages to Be Logged

By default, the trace operation output includes all messages relevant to the logged events.

You can refine the output by including regular expressions that will be matched.

To configure regular expressions to be matched:

- Configure the regular expression.

```
[edit services mobile-ip traceoptions]  
user@host# set file mip_1_logfile_1 match regex
```

- Related Documentation**
- [Tracing Mobile IP Operations for Subscriber Access on page 69](#)

Configuring the Mobile IP Tracing Flags

By default, only important events are logged. You can specify which events and operations are logged by specifying one or more tracing flags.

To configure the flags for the events to be logged:

- Configure the flags.

```
[edit services mobile-ip traceoptions]
```



```
user@host# set flag home-agent
```

Related Documentation • [Tracing Mobile IP Operations for Subscriber Access on page 69](#)

Configuring the Severity Level to Filter Which Mobile IP Messages Are Logged

The messages associated with a logged event are categorized according to severity level. You can use the severity level to determine which messages are logged for the event type. The severity level that you configure depends on the issue that you are trying to resolve. In some cases you might be interested in seeing all messages relevant to the logged event, so you specify **all** or **verbose**. Either choice generates a large amount of output. You can specify a more restrictive severity level, such as **notice** or **info** to filter the messages. By default, the trace operation output includes only messages with a severity level of **error**.

To configure the type of messages to be logged:

- Configure the message severity level.

```
[edit services mobile-ip traceoptions]
user@host# set level severity
```

Related Documentation • [Tracing Mobile IP Operations for Subscriber Access on page 69](#)

Collecting Subscriber Access Logs Before Contacting Juniper Technical Support

Problem When you experience a subscriber access problem in your network, we recommend that you collect certain logs before you contact Juniper Technical Support. This topic shows you the most useful logs for a variety of network implementations. In addition to the relevant log information, you must also collect standard troubleshooting information and send it to Juniper Technical Support in your request for assistance.

Solution To collect standard troubleshooting information:

- Redirect the command output to a file.

```
user@host> request support information | save rsi-1
```

To configure logging to assist Juniper Technical Support:

1. Review the following blocks of statements to determine which apply to your configuration.

[edit]

```
set system syslog archive size 100m files 25
set system auto-configuration traceoptions file filename
set system auto-configuration traceoptions file filename size 100m files 25
set protocols ppp-service traceoptions file filename size 100m files 25
set protocols ppp-service traceoptions level all
set protocols ppp-service traceoptions flag all
set protocols ppp traceoptions file filename size 100m files 25
set protocols ppp traceoptions level all
set protocols ppp traceoptions flag all
set protocols ppp monitor-session all
set interfaces pp0 traceoptions flag all
set demux traceoptions file filename size 100m files 25
set demux traceoptions level all
set demux traceoptions flag all
set system processes dhcp-service traceoptions file filename
set system processes dhcp-service traceoptions file size 100m
set system processes dhcp-service traceoptions file files 25
set system processes dhcp-service traceoptions flag all
set class-of-service traceoptions file filename
set class-of-service traceoptions file size 100m
set class-of-service traceoptions flag all
set class-of-service traceoptions file files 25
set routing-options traceoptions file filename
set routing-options traceoptions file size 100m
set routing-options traceoptions flag all
set routing-options traceoptions file files 25
set interfaces traceoptions file filename
set interfaces traceoptions file size 100m
set interfaces traceoptions flag all
set interfaces traceoptions file files 25
set system processes general-authentication-service traceoptions file filename
set system processes general-authentication-service traceoptions file size 100m
set system processes general-authentication-service traceoptions flag all
set system processes general-authentication-service traceoptions file files 25
```

2. Copy the relevant statements into a text file and modify the log filenames as you want.
3. Copy the statements from the text file and paste them into the CLI on your router to configure logging.
4. Commit the logging configuration to begin collecting information.



.....

NOTE: The maximum file size for DHCP local server and DHCP relay log files is 1 GB. The maximum number of log files for DHCP local server and DHCP relay is 1000.

.....



BEST PRACTICE: Enable these logs only to collect information when troubleshooting specific problems. Enabling these logs during normal operations can result in reduced system performance.

**Related
Documentation**

- *Compressing Troubleshooting Logs from /var/logs to Send to Juniper Technical Support*

CHAPTER 7

Troubleshooting Configuration Statement

traceoptions (Mobile IP)

Syntax	<pre> traceoptions { file <i>filename</i> <files <i>number</i>> <match <i>regular-expression</i> > <size <i>maximum-file-size</i>> <world-readable no-world-readable>; flag <i>flag</i>; level (all error info notice verbose warning); no-remote-trace; } </pre>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> services mobile-ip], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> services mobile-ip], [edit routing-instances <i>routing-instances-name</i> services mobile-ip], [edit services mobile-ip]</p>
Release Information	<p>Statement introduced in Junos OS Release 9.3.</p> <p>Support at the [edit logical-systems <i>logical-system-name</i> ...], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> ...], and [edit routing-instances <i>routing-instances-name</i> ...] hierarchy levels introduced in Junos OS Release 9.5.</p>
Description	Define tracing operations for Mobile IP processes.
Options	<p>file <i>filename</i>— Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory /var/log. Ensure that filenames are unique for each logical system or routing instance in which Mobile IP is configured.</p>



NOTE: Global messages (common to all logical systems and routing instances) are always saved in **/var/log/mipd**. Messages that are specific to a logical system or routing instance are never saved in **/var/log/mipd**. If you do not configure a trace filename for a logical system or routing instance, then nothing is traced for that entity.

files *number*—(Optional) Maximum number of trace files to create before overwriting the oldest one. If you specify a maximum number of files, you also must specify a maximum file size with the **size** option.

Range: 2 through 1000

Default: 3 files

flag *flag*—Tracing operation to perform. To specify more than one tracing operation, include multiple **flag** statements. You can include the following flags:

- **all**—Trace all operations.
- **authentication**—Trace authentication operations.
- **binding**—Trace bindings.

- **event**—Trace events.
- **ha-fsm**—Trace home agent state machine operations.
- **home-agent**—Trace home agent operations.
- **interface-database**—Trace interface database operations.
- **packet**—Trace packet decoding operations.
- **protocol**—Trace protocol operations.
- **rtsock**—Trace routing socket operations.
- **session-db**—Trace session database events.
- **signal**—Trace signal operations.
- **subscriber**—Trace subscriber events.
- **timer**—Trace timer events.
- **trace**—Trace changes in tracing.
- **tunnel**—Trace tunneling operations.
- **user-interface**—Trace user interface events.

level—Specify level of tracing to perform. You can specify any of the following levels:

- **all**—Match all levels.
- **error**—Match error conditions.
- **info**—Match informational messages.
- **notice**—Match notice messages about conditions requiring special handling.
- **verbose**—Match verbose messages.
- **warning**—Match warning messages.

match *regular-expression*—(Optional) Refine the output to include lines that contain the regular expression.

no-remote-trace—Disable remote tracing.

no-world-readable—(Optional) Disable unrestricted file access.

size *maximum-file-size*—(Optional) Maximum size of each trace file. By default, the number entered is treated as bytes. Alternatively, you can include a suffix to the number to indicate kilobytes (KB), megabytes (MB), or gigabytes (GB). If you specify a maximum file size, you also must specify a maximum number of trace files with the **files** option.

Syntax: **size***k* to specify KB, **size***m* to specify MB, or **size***g* to specify GB

Range: 10240 through 1073741824

Default: 128 KB

world-readable—(Optional) Enable unrestricted file access.

Required Privilege	trace—To view this statement in the configuration.
Level	trace-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Tracing Mobile IP Operations for Subscriber Access on page 69

PART 5

Index

- [Index on page 83](#)

Index

Symbols

#, comments in configuration statements.....	xiv
(), in syntax descriptions.....	xiv
< >, in syntax descriptions.....	xiv
[], in configuration statements.....	xiv
{ }, in configuration statements.....	xiv
(pipe), in syntax descriptions.....	xiv

A

AAA	
Mobile IP home agent and	6
access type	
configuring Mobile IP	22
access-type statement	
Mobile IP	24
accounting	
Mobile IP time-based.....	9
accounting methods	
configuring Mobile IP.....	21
algorithm statement	
Mobile IP.....	25
authenticate statement	
Mobile IP.....	26
authentication	
Mobile IP home agent.....	6
authentication attributes	
local Mobile IP.....	20
authentication method	
configuring Mobile IP.....	19

B

binding	
clearing Mobile IP.....	54
braces, in configuration statements.....	xiv
brackets	
angle, in syntax descriptions.....	xiv
square, in configuration statements.....	xiv

C

clear mobile-ip binding command.....	54
comments, in configuration statements.....	xiv

conventions	
text and syntax.....	xiii
curly braces, in configuration statements.....	xiv
customer support.....	xv
contacting JTAC.....	xv

D

documentation	
comments on.....	xv
dynamic home assignment	
configuring Mobile IP.....	21
dynamic-home-assignment statement	
Mobile IP.....	27

E

enable-service statement	
Mobile IP.....	28
entity-type statement	
Mobile IP.....	29

F

font conventions.....	xiii
-----------------------	------

G

generic statement	
Mobile IP.....	29

H

home agent	
configuration overview.....	19
home agent, Mobile IP See Mobile IP home agent	
home-agent statement	
Mobile IP	
dynamic home assignment rule.....	31
IP address rule.....	32
networks.....	30
home-agent-address statement	
Mobile IP.....	33

K

key statement	
Mobile IP.....	34

L

log files	
access to Mobile IP.....	72
collecting for Juniper Technical Support.....	73
configuring Mobile IP trace.....	69
filenames for Mobile IP.....	71

number of Mobile IP.....	71	home-agent	
size of Mobile IP.....	71	dynamic home assignment rule.....	31
M		IP address rule.....	32
manuals		networks.....	30
comments on.....	xv	home-agent-address.....	33
Mobile IP		key.....	34
access type configuration.....	22	mobile-ip.....	35
accounting method.....	21	nai.....	37
authentication method.....	19	order.....	38
binding information, displaying.....	57	peer.....	39
clearing Mobile IP binding.....	54	registration-lifetime.....	40
configuration overview.....	17	replay-method.....	41
dynamic home assignment configuration.....	21	revocation-required.....	42
event log access.....	72	spi.....	43
event logging.....	69	statistics.....	44
filtering trace operation output.....	72	timestamp-tolerance.....	45
flags for tracing operations.....	72	traceoptions.....	46, 78
home agent overview information,		virtual-network.....	49
displaying.....	55	wimax.....	48
home agent traffic information, displaying.....	60	mobile-ip statement	
local authentication attributes.....	20	Mobile IP.....	35
log file size.....	71	N	
log filenames.....	71	nai statement	
message severity levels for tracing		Mobile IP.....	37
operations.....	73	O	
registration request authentication.....	19	order statement	
tracing operations.....	69	Mobile IP.....	38
virtual network information, displaying.....	63	P	
WiMAX Forum Network Architecture release		parentheses, in syntax descriptions.....	xiv
number, displaying.....	65	peer statement	
WiMAX operation.....	22	Mobile IP.....	39
Mobile IP home agent		R	
AAA.....	6	registration	
accounting.....	9	Mobile IP mobile node.....	6
agent discovery.....	3	registration-lifetime statement	
authentication.....	6	Mobile IP.....	40
home address assignment.....	3	replay-method statement	
mobile node registration.....	6	Mobile IP.....	41
overview.....	3	revocation-required statement	
Mobile IP statements		Mobile IP.....	42
access-type.....	24	S	
algorithm.....	25	show mobile-ip home-agent bindings	
authenticate.....	26	command.....	57
dynamic-home-assignment.....	27		
enable-service.....	28		
entity-type.....	29		
generic.....	29		

show mobile-ip home-agent overview	
command.....	55
show mobile-ip home-agent traffic command.....	60
show mobile-ip home-agent virtual-network	
command.....	63
show mobile-ip wimax release command.....	65
spi statement	
Mobile IP.....	43
statistics statement	
access.....	44
support, technical See technical support	
syntax conventions.....	xiii

T

technical support	
collecting logs for.....	73
contacting JTAC.....	xv
time-based accounting	
Mobile IP.....	21
timestamp-tolerance statement	
Mobile IP.....	45
trace operations	
collecting logs for Juniper technical	
support.....	73
filtering output for Mobile IP.....	72
traceoptions statement	
Mobile IP.....	46, 78
tracing operations	
Mobile IP.....	69
troubleshooting subscriber access	
collecting logs for Juniper Technical	
Support.....	73

V

virtual-network statement	
Mobile IP.....	49

W

wimax statement	
Mobile IP.....	48
wireless roaming	
Mobile IP.....	3

