Mobile IPv6 High Availability

Mobile IP is part of both IPv4 and IPv6 standards. Mobile IP allows a host device to be identified by a single IP address even though the device may move its physical point of attachment from one network to another. Regardless of movement between different networks, connectivity at the different points is achieved seamlessly without user intervention. Roaming from a wired network to a wireless or wide-area network is also done with ease. Mobile IP provides ubiquitous connectivity for users, whether they are within their enterprise networks or away from home.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About Mobile IPv6 High Availability

Mobile IPv6 Tunnel Optimization

Mobile IPv6 tunnel optimization enables routing over a native IPv6 tunnel infrastructure, allowing Mobile IPv6 to use all IPv6 tunneling infrastructure features, such as Cisco Express Forwarding switching support.

After the home agent receives a valid BU request from a mobile node, it sets up its endpoint of the bidirectional tunnel. This process involves creating a logical interface with the encapsulation mode set to IPv6/IPv6, the tunnel source to the home agent's address on the mobile node's home link, and the tunnel destination set to the mobile node's registered care-of address. A route will be inserted into the routing table for the mobile node's home address via the tunnel.

IPv6 Host Group Configuration

Users can create mobile user or group policies using the IPv6 host group configuration. The host group profile lookup interface will allow the lookup of the profile associated with the sender of the BU using any of the search keys:

- Profile name
- IPv6 address
- Network address identifier (NAI)

The host profile lookup interface also specifies the authentication properties for the IPv6 mobile node by creating either a unidirectional or bidirectional security parameter index (SPI).

A group profile is activated after the SPI option is configured and either an NAI or an IPv6 address is configured. In addition, a profile is deactivated if the minimum required options are not configured. If any active profile that has active bindings gets deactivated or removed, all bindings associated to that profile are revoked.

Mobile IPv6 Node Identification Based on NAI

A mobile node can identify itself using its home address as an identifier. The Mobile IPv6 protocol messages use this identifier in their registration messages. However, for certain deployments it is essential that the mobile node has the capability to identify itself using a logical identifier, such as NAI, rather than a network address. The mobile node identifier option for Mobile IPv6 allows a mobile node to be identified by NAI rather than IPv6 address. This feature enables the network to give a dynamic IPv6 address to a mobile node and authenticate the mobile node using authentication, authorization, and accounting (AAA). This option should be used when either Internet Key Exchange (IKE) or IPsec is not used for protecting BUs or binding acknowledgments (BAs).

In order to provide roaming services, a standardized method, such as NAI or a mobile node home address, is needed for identifying users. Roaming may be loosely defined as the ability to use any one of multiple Internet service providers (ISPs) while maintaining a formal, customer-vendor relationship with only one. Examples of where roaming capabilities might be required include ISP confederations and ISP-provided corporate network access support. Other entities interested in roaming capability may include the following:

- Regional ISPs, operating within a particular state or province, that want to combine efforts with those of other regional providers to offer dialup service over a wider area.
- National ISPs that want to combine their operations with those of one or more ISPs in another country to offer more comprehensive dialup service in a group of countries or on a continent.
- Wireless LAN hot spots that provide service to one or more ISPs.
- Businesses that want to offer their employees a comprehensive package of dialup services on a global basis. Those services may include Internet access and secure access to corporate intranets using a VPN.

Authentication Protocol for Mobile IPv6

The authentication protocol for Mobile IPv6 support secures mobile node and home agent signaling using the MN-HA mobility message authentication option, which authenticates the BU and BA messages based on the shared-key-based security association between the mobile node (MN) and the HA. This feature allows Mobile IPv6 to be deployed in a production environment where a non-IPsec authentication method is required. MN-HA consists of a mobility SPI, a shared key, an authentication algorithm, and the mobility message replay protection option.

The mobility SPI is a number from 256 through 4,294,967,296. The key consists of an arbitrary value and is 16 octets in length. The authentication algorithm used is HMAC_SHA1. The replay protection mechanism may use either the sequence number option or the time-stamp option. The MN-HA mobility message authentication option must be the last option in a message with a mobility header if it is the only mobility message authentication option in the message.

When a BU or BA message is received without the MN-HA option and the entity receiving it is configured to use the MN-HA option or has the shared-key-based mobility security association for the mobility message authentication option, the entity discards the received message.

The mobility message replay protection option allows the home agent to verify that a BU has been freshly generated by the mobile node and not replayed by an attacker from some previous BU. This functionality is especially useful for cases where the home agent does not maintain stateful information about the mobile node after the binding entry has been removed. The home agent performs the replay protection check after the BU has been authenticated. The mobility message replay protection option is used by the mobile node for matching the BA with the BU. When the home agent receives the mobility message replay protection option in BU, it must include the mobility message replay protection option in the BA.

How to Configure Mobile IPv6 High Availability

Verifying Native IPv6 Tunneling for Mobile IPv6

Using the native IPv6 tunneling (or generic routing encapsulation [GRE]) infrastructure improves the scalability and switching performance of the home agent. After the home agent sends a BU from a mobile node, a tunnel interface is created with the encapsulation mode set to IPv6/IPv6, the source address set to that of the home agent address on the home interface of the mobile node, and the tunnel destination set to that of the CoA of the mobile node.

These features are transparent and need not be configured in order to work with Mobile IPv6. For further information on IPv6 tunneling and how to implement GRE tunneling in IPv6, see the *Implementing Tunneling for IPv6* module.

SUMMARY STEPS

1. **enable**
2. **show ipv6 mobile tunnels** [**summary** | **tunnel** *if-number*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show ipv6 mobile tunnels** [**summary** | **tunnel** *if-number* **Example:** `Router# show ipv6 mobile tunnels`	Lists the Mobile IPv6 tunnels on the home agent.

Configuring and Verifying Host Groups for Mobile IPv6

Users can create mobile user or group policies using the host group configuration. The host group profile lookup interface will allow the lookup of the profile associated with the sender of the BU using the sender's profile name, IPv6 address, or NAI. The host profile lookup interface also specifies the authentication properties for the IPv6 mobile node by creating either a unidirectional or bidirectional SPI.

A mobile node can identify itself using its profile name or home address as an identifier, which the Mobile IPv6 protocol messages use as an identifier in their registration messages. However, for certain deployments it is essential that the mobile node has the capability to identify itself using a logical identifier such as NAI rather than a network address.

Note

- You cannot configure two host group profiles with the same IPv6 address when using the IPv6 address option.
- You cannot configure a profile with the NAI option set to a realm name and the address option set to a specific IPv6 address. You can either remove the NAI option or specify a fully qualified user name for the NAI option.

>

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 mobile home-agent**
4. **binding** [**access** *access-list-name* | *auth-option* | *seconds*| *maximum* | *refresh*
5. **host group** *profile-name*
6. **address** {*ipv6-address* | **autoconfig**
7. **nai realm** | **user** | **macaddress**] {*user* **@** *realm*| **@** *realm*
8. **authentication inbound-spi** {*hex-in* | **decimal** *decimal-in*} **outbound-spi** {*hex-out* | **decimal** *decimal-out*} | **spi** {*hex-value* | **decimal** *decimal-value*}} **key** {**ascii** *string* | **hex** *string*}[**algorithm** *algorithm-type*] [**replay within** *seconds*
9. **exit**
10. **exit**
11. **show ipv6 mobile host groups** *profile-name*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ipv6 mobile home-agent** **Example:** `Router(config)# ipv6 mobile home-agent`	Places the router in home-agent configuration mode.
Step 4	**binding** [**access** *access-list-name*	*auth-option*	*seconds*| *maximum*	*refresh* **Example:** `Router(config-ha)# binding 15`	Configures binding options for the Mobile IPv6 home agent feature.
Step 5	**host group** *profile-name* **Example:** `Router(config-ha)# host group profile1`	Creates a host configuration in Mobile IPv6. • Multiple instances with different profile names can be created and used.

	Command or Action	Purpose
Step 6	**address** {*ipv6-address* | **autoconfig** **Example:** `Router(config-ha)# address baba 2001:DB8:1`	Specifies the home address of the IPv6 mobile node.
Step 7	**nai realm** | **user** | **macaddress**] {*user* **@** *realm*| **@** *realm* **Example:** `Router(config-ha)# nai @cisco.com`	Specifies the NAI for the IPv6 mobile node.
Step 8	**authentication inbound-spi** {*hex-in* | **decimal** *decimal-in*} **outbound-spi** {*hex-out* | **decimal** *decimal-out*} | **spi** {*hex-value* | **decimal** *decimal-value*}} **key** {**ascii** *string* | **hex** *string*}[**algorithm** *algorithm-type*] [**replay within** *seconds* **Example:** `Router(config-ha)# authentication spi 500 key ascii cisco`	Specifies the authentication properties for the IPv6 mobile node by creating either a unidirectional or bidirectional SPI.
Step 9	**exit** **Example:** `Router(config-ha)# exit`	Exits home-agent configuration mode, and returns the router to global configuration mode.
Step 10	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode, and returns the router to privileged EXEC mode.
Step 11	**show ipv6 mobile host groups** *profile-name*] **Example:** `Router# show ipv6 mobile host groups`	Displays information about Mobile IPv6 host groups.

Configuration Examples for Mobile IPv6 High Availability

Example Configuring Host Groups for Mobile IPv6

The following example shows how to configure a Mobile IPv6 host group named group1:

```
ipv6 mobile host group group1

  nai sri@cisco.com

  address autoconfig

  authentication spi 500 key ascii cisco
```

Additional References

Related Documents

Related Topic	Document Title
IPv6 addressing and connectivity	*IPv6 Configuration Guide*
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
IPv6 commands	*Cisco IOS IPv6 Command Reference*
Cisco IOS IPv6 features	*Cisco IOS IPv6 Feature Mapping*

Standards and RFCs

Standard/RFC	Title
RFCs for IPv6	*IPv6 RFCs*

MIBs

MIB	MIBs Link
	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Mobile IPv6 High Availability

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to . An account on Cisco.com is not required.

Table 1: Feature Information for Mobile IPv6 High Availability

Feature Name	Releases	Feature Information
Mobile IPv6 High Availability	12.4(11)T	This phase of development for Mobile IPv6 includes support for NAI, alternate authentication, and native IPv6 tunnel infrastructure. The following commands were introduced or modified: **address**, **authentication**, **binding**, **host group**, **ipv6 mobile home-agent**, **nai**, **show ipv6 mobile host groups**, **show ipv6 mobile tunnels**.