Mobile IP Dynamic Security Association and Key Distribution

The Mobile IP Dynamic Security Association and Key Distribution feature enables a Mobile IP client (mobile node) to use the Microsoft Windows login information to generate the dynamic shared keys needed to create the security associations between it and the home agent. These security associations are used to authenticate the mobile device. In response to a successful registration, basic configuration parameters such as the DHCP server address, home address prefix length, and domain name system (DNS) address are also passed on to the mobile node in the form of extensions to the registration reply message sent by the home agent.

This feature eliminates the need for any configuration of the Mobile IP client software once it is installed. Now customers need not log in and authenticate multiple times, making the Mobile IP client software a "plug-and-play" operation.

Feature History for the Mobile IP Dynamic Security Association and Key Distribution Feature

Release	Modification
12.3(4)T	This feature was introduced.

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.

Prerequisites for Mobile IP Dynamic Security Association and Key Distribution

Your network must be configured to run Mobile IP. The home agent must be configured with the authentication, authorization, and accounting (AAA) address of a RADIUS server that has access to the domain controller for authenticating the user in the Windows domain.

Because Mobile IP requires support on the host device, each mobile node must be appropriately configured for the desired Mobile IP service with client software.

Restrictions for Mobile IP Dynamic Security Association and Key Distribution

This feature can be used only in a Windows operating system environment.

Information About Mobile IP Dynamic Security Association and Key Distribution

Session Identifiers

This feature introduces the concept of a session identifier (session-id) that is available if a network access identifier (NAI) is specified in your configuration. The session identifier is optional and can be added by the mobile node in the initial registration request. For example, a single user can have multiple sessions (for example when logging through different devices such as a PDA, cellular phone, or laptop) and use the same NAI for all sessions. These individual sessions are identified by the session identifier. If the session identifier is present in the initial registration, it must be present in all subsequent registration renewals from the mobile node.

Using the Cisco Secure ACS Server

Because this feature leverages an existing authentication infrastructure, such as the Windows Domain Controller (DC) database or Active Directory (AD), you need not configure any Mobile IP client user information in a AAA server. You only need to configure the AAA so it can use the DC/AD to authenticate the Mobile IP client users upon receiving a RADIUS request from a home agent.

The following is a brief summary of the steps necessary to configure the Cisco Secure Access Control Server (ACS) to use a database to authenticate Mobile IP clients.

- In the navigation bar, click External User Databases. Select Windows Domain Database to authenticate unknown users.
- In the navigation bar, click External User Databases. Map the domain of the unknown users to an ACS group.
- Click Database Group Mappings. Check the Microsoft MPPE Key attribute for the mapped ACS group.

For more information on Cisco Secure ACS configuration, refer to the "Administering External User Databases" chapter of the *Cisco Secure ACS Windows Server 3.1 User Guide*.

Benefits of Mobile IP Dynamic Security Association and Key Distribution

- This feature eliminates the need for any configuration of the Mobile IP client software once it is installed. Now customers need not log in and authenticate multiple times, making the Mobile IP client software a "plug-and-play" operation.
- For network administrators, this feature simplifies Mobile IP provisioning and increases mobility security through dynamic re-keying.

Additional References

The following sections provide references related to the Mobile IP Dynamic Security Association and Key Distribution feature.

Related Documents

Related Topic	Document Title
Mobile IP commands: complete command syntax, command mode, defaults, usage guidelines, and examples	*Cisco IOS IP Command Reference, Volume 4 of 4: IP Mobility,* Release 12.3 T
Information about Network Access Identifiers in Mobile IP	http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftnaiadd.htm Mobile IP Generic NAI Support and Home Address Allocation feature document, Release 12.2(13)T
Configuration tasks for Cisco Secure ACS	http://www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/csacs4nt/acs31/acsuser/acs31ug.pdf Cisco Secure ACS Windows Server 3.1 User Guide

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	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

RFCs

RFCs	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	--

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/public/support/tac/home.shtml

Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS IP Mobility Command Reference* at http://www.cisco.com/en/US/docs/ios/ipmobility/command/reference/imo_book.html. For information about all Cisco IOS commands, go to the Command Lookup Tool at http://tools.cisco.com/Support/CLILookup or to the *Cisco IOS Master Commands List* .

- **clear ip mobile binding**

- **clear ip mobile visitor**
- **show ip mobile binding**
- **show ip mobile visitor**

Glossary

home agent --A router on a home network of the mobile node or that tunnels packets to the mobile node or mobile router while it is away from home. It keeps current location information for registered mobile nodes called a mobility binding.

mobile node --A host or router that changes its point of attachment from one network or subnet to another. A mobile node may change its location without changing its IP address; it may continue to communicate with other Internet nodes at any location using its home IP address, assuming that link-layer connectivity to a point of attachment is available.

NAI--network access identifier. The user ID submitted by the mobile node during registration to identify the user for authentication. The NAI might help route the registration request to the correct home agent.

Note Refer to Internetworking Terms and Acronyms for terms not included in this glossary.