Mobile IP Challenge and Response Extensions

The Mobile IP--Challenge/Response Extensions feature enables a foreign agent (FA) to authenticate a mobile node (MN) by sending mobile foreign challenge extensions (MFCE) and mobile node-AAA authentication extensions (MNAE) to the home agent (HA) in registration requests.

Feature Specifications for Mobile IP--Challenge/Response Extensions

Feature History	
Release	Modification
12.2(13)T	This feature was introduced.
Supported Platforms	
For platforms supported in Cisco IOS Release 12.2(13)T, consult Cisco Feature Navigator.	

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 Challenge Response Extensions

In the Mobile IP--Challenge/Response Extensions feature, the foreign agent expects mobile node RRQs to contain the following extensions:

- Mobile node network address identifier
- MHAE
- Mobile node-foreign agent challenge extension
- Mobile node-AAA extension authenticator computed based on a shared secret between the mobile node and the AAA server.

If unique per-user passwords are configured on the AAA and the mobile nodes, and the mobile node or home agent security association is configured on the AAA server, the HA expects mobile node RRQs received from the FA CoA to contain the following:

- MFCE
- Mobile node -AAA extension authenticator

Restrictions for Mobile IP Challenge Response Extensions

The Mobile IP--Challenge/Response Extensions feature has the following restrictions:

- Mobile Node Colocated care-of address (CCOA) mode is not supported.

Information About Foreign Agent Challenge Response Extensions

Challenge Response Extensions

Mobile IP, as originally implemented, defines a Mobile-Foreign Authentication extension by which a mobile node can authenticate itself to a foreign agent. This Mobile-Foreign Authentication extension does not provide complete replay protection for the foreign agent and does not allow the foreign agent to use existing methods, such as Challenge Handshake Authentication Protocol (CHAP) to authenticate a mobile node. The Mobile IP--Foreign Agent Challenge/Response Extensions feature extends the Mobile IP agent advertisements and the registration requests that enable a foreign agent to use a challenge/response mechanism to authenticate a mobile node.

When the Mobile IP--Foreign Agent Challenge/Response Extensions feature is configured, the foreign agent expects the mobile node to include a challenge extension with a challenge value that the mobile node had previously advertised. The foreign agent also expects to receive this challenge extension within a specific time interval. The mobile node must also send an extension for authentication (MFAE or MN-AAA.)

How to Configure Foreign Agent Challenge Response Extensions

Configuring FA Challenge Response Extensions

Perform this task to configure a foreign agent to authenticate a mobile node by sending MFCEs and MNAEs in registration requests.

Before You Begin

If unique per-user passwords are configured on the AAA and the mobile nodes, and the mobile node or home agent security association is configured on the AAA server, the HA expects mobile node RRQs received from the FA CoA to contain the following:

- MFCE
- Mobile node -AAA extension authenticator

If the MFCE and MN-AAA extension authenticator are not forwarded to the home agent, the AAA server storing the mobile node/ home agent SAs must have identical passwords for all users to aid SA retrieval.

Note If the Mobile Node is registering in FA-COA mode and the Security Associations (SAs) must be obtained from AAA, the user password must be configured as "cisco".

SUMMARY STEPS

1. **enable**
2. **configure** {**terminal** | **memory** | **network**}
3. **router mobile**
4. **ip mobile foreign-agent care-of** *interface*
5. **interface** *type number*
6. **ip address** *ip-address mask*
7. **ip irdp**
8. **ip irdp holdtime** *seconds*
9. **ip irdp maxadvertinterval** *seconds*
10. **ip irdp minadvertinterval** *seconds*
11. **ip mobile foreign-service challenge** {**timeout** *value* | **window** *number*}
12. **ip mobile foreign-service challenge**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables higher privilege levels, such as privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure** {**terminal** | **memory** | **network**} **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**router mobile** **Example:** `Router(config)# router mobile`	Enables Mobile IP on the router.
Step 4	**ip mobile foreign-agent care-of** *interface* **Example:** `Router(config)# ip mobile foreign-agent care-of serial0`	Enables Foreign Agent services when at least one care-of address is configured. • This is the foreign network termination point of the tunnel between the Foreign Agent and Home Agent. The care-of address is the IP address of the interface. The interface, whether physical or loopback, need not be the same as the visited interface.
Step 5	**interface** *type number* **Example:** `Router(config)# interface serial0`	Configures an interface and enters interface configuration mode.
Step 6	**ip address** *ip-address mask* **Example:** `Router(config-if)# ip address 10.1.0.1 255.255.255.255`	Sets a primary IP address of the interface.
Step 7	**ip irdp** **Example:** `Router(config-if)# ip irdp`	Enables IRDP processing on an interface.
Step 8	**ip irdp holdtime** *seconds*	Length of time in seconds that advertisements are held valid.

	Command or Action	Purpose
	Example: `Router(config-if)# ip irdp holdtime 9000`	• Default is three times the **maxadvertinterval**period. When foreign agent challenge extensions are implemented, this value must be set to 9000 seconds.
Step 9	**ip irdp maxadvertinterval** *seconds* **Example:** `Router(config-if)# ip irdp maxadvertinterval 9000`	(Optional) Specifies the maximum interval in seconds between advertisements.
Step 10	**ip irdp minadvertinterval** *seconds* **Example:** `Router(config-if)# ip irdp minadvertinterval 7`	(Optional) Specifies the minimum interval in seconds between advertisements.
Step 11	**ip mobile foreign-service challenge** {**timeout** *value* | **window** *number*} **Example:** `Router(config-if)# ip mobile foreign-service challenge timeout 10`	Enables Foreign Agent service on an interface. • Configures the challenge timeout value and the number of valid recently sent challenge values.
Step 12	**ip mobile foreign-service challenge** **Example:** **forward-mfce** **Example:** `Router(config-if)# ip mobile foreign-service challenge forward-mfce`	Enables the foreign agent to send MFCEs to the home agent in registration requests.

Verifying Foreign Agent Service Configuration

Perform this task to optionally verify that the interface has been configured to provide foreign agent services.

SUMMARY STEPS

1. **enable**
2. **show ip mobile globals**
3. **show ip mobile interface**
4. **show ip mobile traffic**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables higher privilege levels, such as privileged EXEC mode. Enter your password if prompted.
Step 2	**show ip mobile globals** **Example:** `Router# show ip mobile globals`	(Optional) Displays global information for mobile agents.
Step 3	**show ip mobile interface** **Example:** `Router# show ip mobile interface`	(Optional) Displays advertisement information for interfaces that are providing foreign agent service or are home links for mobile nodes.
Step 4	**show ip mobile traffic** **Example:** `Router# show ip mobile traffic`	(Optional) Displays protocol counters.

Additional References

The following sections provide additional references related to the Mobile IP--Challenge/Response Extensions feature:

Related Documents

Related Topic	Document Title
Authentication	The part " Authentication, Authorization, and Accounting (AAA)" in the Cisco IOS Security Configuration Guide, Release 12.2

Related Topic	Document Title
IKE and IPSec security protocols	The part " IP Security and Encryption" in the Cisco IOS Security Configuration Guide, Release 12.2
Mobile IP	Introduction to Mobile IP
Cisco mobile networks	Cisco Mobile Networks
Mobile wireless configuration	Cisco IOS Mobile Wireless Configuration Guide, Release 12.2
Mobile wireless commands	Cisco IOS Mobile Wireless Command Reference, Release 12.2

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[1]	MIBs Link
• RFC2006-MIB • CISCO-MOBILE-IP-MIB	To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL: http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

1 Not all supported MIBs are listed.

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

http://tools.cisco.com/ITDIT/MIBS/servlet/index

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

To access Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random

password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

http://www.cisco.com/register

RFCs

RFCs[2]	Title
RFC 2002	IP Mobility Support
RFC 2003	IP Encapsulation within IP
RFC 2005	Applicability Statement for IP Mobility Support
RFC 2006	The Definitions of Managed Objects for IP Mobility Support
RFC 3024	*Reverse Tunneling for Mobile IP, revised*

2 Not all supported RFCs are listed.

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, tools, and lots more. 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* .

- **debug ip mobile advertise**
- **ip mobile foreign-service**
- **show ip mobile traffic**