Mobile IP MIB Support for SNMP

This document describes the Mobile IP MIB Support for SNMP feature in Cisco IOS Release 12.2(2)T. It includes the following sections:

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.

Feature Overview

The Mobile IP MIB Support for SNMP feature adds a MIB module that expands network monitoring and management capabilities of foreign agent (FA) and home agent (HA) Mobile IP entities. Mobile IP management using Simple Network Management Protocol (SNMP) is defined in two MIBs: the RFC2006-MIB and the CISCO-MOBILE-IP-MIB.

The RFC2006-MIB is a MIB module that uses the definitions defined in RFC 2006, *The Definitions of Managed Objects for IP Mobility Support Using SMIv2*. Beginning in Cisco IOS Release 12.2(1)T, RFC 2006 Set operations and an SNMP notification (trap) are supported. Set operations, performed from a network management system (NMS), allow you to use the RFC2006-MIB objects for starting and stopping the Mobile IP service, modifying and deleting security associations, modifying advertisement parameters, and configuring 'care-of addresses' for FAs. An SNMP notification for security violations can also be enabled on supported routing devices using the Cisco IOS software (see the Configuration Tasks, on page 5 section for details).

The CISCO-MOBILE-IP-MIB is a Cisco enterprise-specific extension to the RFC2006-MIB. The CISCO-MOBILE-IP-MIB allows you to monitor the total number of HA mobility bindings and the total number of FA visitor bindings using an NMS. These bindings are defined in the CISCO-MOBILE-IP-MIB as *cmiHaRegTotalMobilityBindings* and *cmiFaRegTotalVisitors* , respectively.

Benefits

The RFC2006-MIB defines a notification for Mobile IP entities (HA or FA) that can be sent to an NMS if there is a security violation. This notification can be used to identify the source of intrusions.

The RFC2006-MIB also defines a table (mipSecViolationTable) to log the security violations in the Mobile IP entities. This log can be retrieved from an NMS (using Get operations) and can be used to analyze the security violation instances in the system.

The CISCO-MOBILE-IP-MIB allows you to monitor the total number of HA mobility bindings. Customers can now obtain a snapshot of the current load in their HAs, which is important for gauging load at any time in the network and tracking usage for capacity planning.

Restrictions

The following restrictions exist for using Set operations on the following objects and tables in the RFC2006 MIB:

- mipEnable object--This object can be used to start and stop the Mobile IP service on the router. There are no issues with the Set support for this object.
- faRegistrationRequired object--This object controls whether the mobile node (MN) should register with the FA. The Cisco implementation of Mobile IP allows configuring this parameter at an interface level through the command line interface. However, this object is not defined at the interface level in the MIB. Therefore, Set support is not enabled for this object.
- mipSecAssocTable--This table allows the configuration of security associations between different Mobile IP entities (HA, FA, and MN). The index objects for this table are the IP address of the entity and security parameter index (SPI). To create a security association, the Cisco IOS software needs to know the correspondence between the IP address of the entity (used as index) and the kind of entity (FA, HA, or MN). No object in this table provides this information. Therefore, creation of rows in this table is not supported. The Cisco implementation allows only the modification of existing security associations. The table below shows the fixed values for objects in the mipSecAssocTable.

Table 1: Fixed Security Method for RFC2006-MIB mipSecAssocTable Objects

Object	Fixed Security Method Value
mipSecAlgorithmType	MD5

Object	Fixed Security Method Value
mipSecAlgorithmMod	prefixSuffix
mipSecReplayMethod	timestamps

When the mipSecKey object value is set with a Set operation, the value will be interpreted as an ASCII key if it contains printable ASCII values. Otherwise, the key will be interpreted as a hex string.

Because there is no rowStatus object in this table, deletion of rows in this table is achieved by setting the mipSecKey object to some special value. Existing security associations can be removed by setting the mipSecKey object to all zeros.

- maAdvConfigTable--This table allows modification of advertisement parameters of all advertisement interfaces in the mobility agent. Even though this table has a rowStatus object, row creation and destroy is not possible because creating a new row implies that an HA or FA service should be started on the interface corresponding to the new row. But no object in this table specifies the service (HA or FA) to be started. Therefore, there should already be one row corresponding to each interface on which the FA or HA service is enabled.

When the maAdvResponseSolicitationOnly object has a TRUE value, the maAdvMaxInterval, maAdvMinInterval, and maAdvMaxAdvLifetime objects of this table are not instantiated.

If the interface corresponding to a row is not up, the row will move to the notReady state.

- faCOATable--This table allows configuration of care-of addresses on an FA. This table has two objects: the rowStatus object and the index of the table. Row creation is not supported through createAndWait rowStatus because this table has only one object that can be set (rowStatus). The notInService state for rows in this table is not supported.

If the interface corresponding to the care-of address (configured by a row of this table) is not up, then the status of the row will be notReady. Creating a new row that corresponds to an interface that is not up is not possible.

Related Features and Technologies

- SNMP
- Mobile IP

Related Documents

This feature adds support for RFC 2006 Set operations and security violation traps. For specifications, see RFC 2006, *The Definitions of Managed Objects for IP Mobility Support Using SMIv2.*

For information on configuring SNMP using Cisco IOS software, refer to the following documents:

- The " Configuring SNMP Support" chapter of the *Cisco IOS Configuration Fundamentals Configuration Guide,* Release 12.2

- The " SNMP Commands" chapter of the *Cisco IOS Configuration Fundamentals Command Reference,* Release 12.2

For information on using SNMP MIB features, refer to the appropriate documentation for your network management system.

For information on configuring Mobile IP using Cisco IOS software, refer to the following documents:

- The " Configuring Mobile IP" chapter of the *Cisco IOS IP Configuration Guide,* Release 12.2
- The " Mobile IP Commands" chapter of the *Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services,* Release 12.2

Supported Platforms

Mobile IP support for SNMP functionality is available only in software images that support Mobile IP and SNMP. Supported platforms include the following:

- Catalyst 5000 family Route Switch Module (RSM)
- Catalyst 6000 family Multilayer Switch Feature Card (MSFC)
- Cisco 2600 series
- Cisco 3600 series
- Cisco 4000 series
- Cisco 7000 family (Cisco 7100 series, 7200 series, and 7500 series)
- Cisco uBR7200 series

Supported Standards MIBs and RFCs

Standards

No new or modified standards are supported by this feature.

MIBs

- 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 .

RFCs

- RFC 2006, *The Definitions of Managed Objects for IP Mobility Support Using SMIv2*
- RFC 2002, *IP Mobility Support*

Prerequisites

The tasks in this document assume that you have configured SNMP and Mobile IP on your devices. Because this feature allows modification and deletion of security associations in the mipAssocTable through SNMP Set operations, use of SNMPv3 is strongly recommended.

Configuration Tasks

Configuring the Router to Send Mobile IP MIB Notifications

To configure the router to send Mobile IP traps or informs to a host, use the following commands in global configuration mode. Note that Mobile IP notifications need not be enabled on a system to process simple Set or Get SNMP requests.

Command	Purpose
`Router(config)#` **snmp-server enable traps ipmobile**	Enables the sending of Mobile IP notifications (traps and informs) for use with SNMP.
`Router(config)#` **snmp-server host** *host-addr* [**traps** | **informs**][**version** {**1** | **2c** | **3** [**auth** | **noauth** | **priv**]}] *community-string* [**udp-port** *port*] **ipmobile**	Specifies the recipient (host) for Mobile IP traps or informs.

Verifying Mobile IP MIB Configuration

Use the **more system:running-config** or the **show running-config** command to verify that the desired snmp-server commands are in your configuration file.

Monitoring and Maintaining Mobile IP MIBs

The Mobile IP MIB Support for SNMP feature is designed to provide information to network management applications (typically graphical-user-interface programs running on an external NMS). Mobile IP MIB objects can be read by the NMS using SNMP Set, Get, Get-next, and Get-bulk operations. Traps or informs can also be sent to the NMS by enabling the "ipmobile" notification type as described in the Configuration Tasks, on page 5 section.

Configuration Examples

In the following example, Mobile IP security violation notifications are sent to the host myhost.cisco.com as informs. The community string is defined as private1.

```
snmp-server enable traps ipmobile
snmp-server host myhost.cisco.com informs version 3 auth private1
```

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* .

New Command

- **snmp-server enable traps ipmobile**

Modified Command

- **snmp-server host**

Glossary

care-of address --An address used temporarily by a mobile node as a tunnel exit-point when the mobile node is connected to a foreign link.

foreign agent --A router on a visited network of a mobile node that provides routing services to the mobile node while registered. The foreign agent detunnels and delivers datagrams to the mobile node that were tunneled by the home agent of the mobile node. For datagrams sent by a mobile node, the foreign agent may serve as a default router for registered mobile nodes.

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

inform --An SNMP trap message that includes a delivery confirmation request. See "trap."

MIB --Management Information Base. Database of network management information that is used and maintained by a network management protocol such as SNMP. The value of a MIB object can be changed or retrieved using SNMP commands, usually through a Network Management System (NMS). MIB objects are organized in a tree structure that includes public (standard) and private (proprietary) branches.

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 link-layer connectivity to a point of attachment is available.

NMS --network management system. An application or suite of applications designed to monitor networks using SNMP. CiscoView is one example of an NMS.

SNMP --Simple Network Management Protocol. Management protocol used almost exclusively in TCP/IP networks. SNMP provides a means to monitor and control network devices, and to manage configurations, statistics collection, performance, and security, typically through the use of an NMS.

SPI --security parameter index. The index identifying a security context between a pair of nodes.

trap --Message sent by an SNMP agent to a network management station, console, or terminal to indicate the occurrence of a significant event, such as a specifically defined condition or a threshold that was reached.