MIB Support

This chapter describes the MIBs supported by Cisco 3200 Series Mobile Access Routers.

General MIBs

- BRIDGE-MIB
- CISCO-BULK-FILE-MIB
- CISCO-CDP-MIB
- CISCO-CIRCUIT-INTERFACE-MIB
- CISCO-CONFIG-COPY-MIB
- CISCO-CONFIG-MAN-MIB
- CISCO-ENVMON-MIB
- CISCO-FLASH-MIB
- CISCO-FTP-CLIENT-MIB
- CISCO-IMAGE-MIB
- CISCO-MEMORY-POOL-MIB
- CISCO-NTP-MIB
- CISCO-NBAR-PROTOCOL-DISCOVERY-MIB
- CISCO-PROCESS-MIB
- CISCO-STACKMAKER-MIB
- CISCO-SYSLOG-MIB
- ENTITY-MIB
- IF-MIB
- OLD-CISCO-CHASSIS-MIB
- OLD-CISCO-CPU-MIB
- OLD-CISCO-FLASH-MIB
- OLD-CISCO-INTERFACES-MIB
- OLD-CISCO-MEMORY-MIB

- OLD-CISCO-SYS-MIB
- OLD-CISCO-SYSTEM-MIB
- RFC 1213-MIB (MIBII)
- SNMPv2-MIB

Wireless MIBs

- IEEE802dot11-MIB
- Q-BRIDGE-MIB
- P-BRIDGE-MIB
- CISCO-DOT11-IF-MIB
- CISCO-WLAN-VLAN-MIB
- CISCO-IETF-DOT11-QOS-MIB
- CISCO-IETF-DOT11-QOS-EXT-MIB
- CISCO-DOT11-ASSOCIATION-MIB
- CISCO-DDP-IAPP-MIB
- CISCO-IP-PROTOCOLFILTER-MIB
- CISCO-SYSLOG-EVENTEXT-MIB
- CISCO-TBRIDGE-DEV-IFMIB

Routing and Routed Protocol MIBs

- CISCO-MOBILE-IP-MIB
- CISCO-PING-MIB
- CISCO-TCP-MIB
- OLD-CISCO-IP-MIB
- OLD-CISCO-TCP-MIB
- RFC 1253-MIB (OSPF)
- TCP-MIB
- UDP-MIB
- RFC 2006-MIB
- BGP4-MIB
- CISCO-BGP4-MIB

LAN and WAN MIBs

- RFC 1398-MIB (Ethernet)
- CISCO-DIAL-CONTROL-MIB
- CISCO-FRAME-RELAY-MIB
- RFC 1315-MIB (Frame Relay)
- RFC 1381-MIB (LAPB)
- RFC1382-MIB (X.25)
- RS-232-MIB

IP Multicasting MIBs

- CISCO-IPMROUTE-MIB
- CISCO-PIM-MIB
- IGMP-STD-MIB
- IPMROUTE-MIB
- IPMROUTE-STD-MIB
- MSDP-MIB
- PIM-MIB

IPSEC/VPN MIBs

- CISCO-IPSEC-MIB
- CISCO-IPSEC-FLOW-MONITOR-MIB
- CISCO-IPSEC-POLICY-MAP-MIB
- CISCO-VPDN-MGMT-MIB

QOS MIBs

- CISCO-CAR-MIB
- CISCO-IP-STAT-MIB
- CISCO-QUEUE-MIB
- INT-SERV-MIB
- INT-SERV-GUARANTEED-MIB
- RSVP-MIB
- CISCO-CLASS-BASED-QOS-MIB
- CISCO-PPPOE-MIB

Network Management MIB

- CISCO-RTTMON-MIB

VLAN MIBs

- CISCO- VLAN-MEMBERSHIP-MIB
- CISCO-VTP-MIB
- CISCO-VLAN-IFTABLE-RELATIONSHIP-MIB

Mobile IP MIB Support

The Mobile IP MIB support for the Simple Network Management Protocol (SNMP) feature adds a MIB module that expands network monitoring and management capabilities of foreign agent and home agent Mobile IP entities. Mobile IP management using SNMP is defined in two MIBs: the RFC 2006-MIB and the CISCO-MOBILE-IP-MIB.

The RFC 2006-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 RFC 2006-MIB objects for starting and stopping the Mobile IP service, modifying and deleting security associations, modifying advertisement parameters, and configuring care-of addresses for foreign agents. An SNMP notification for security violations can also be enabled on supported routing devices using the IOS software.

The CISCO-MOBILE-IP-MIB is a Cisco enterprise-specific extension to the RFC 2006-MIB. The CISCO-MOBILE-IP-MIB allows you to monitor the total number of home agent mobility bindings and the total number of foreign agent visitor bindings using an NMS. These bindings are defined in the CISCO-MOBILE-IP-MIB as *cmiHaRegTotalMobilityBindings* and *cmiFaRegTotalVisitors*, respectively.

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.

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

Mobile IP MIB Benefits

The RFC 2006-MIB defines a notification for Mobile IP entities (home agent or foreign agent) 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 RFC 2006-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 home agent 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.

Mobile IP MIB Restrictions

The following restrictions exist for using Set operations on the following objects and tables in the RFC 2006 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 should register with the foreign agent. 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, no SNMP operation is permitted on this object.
- mipSecAssocTable—This table allows the Management Station to view/modify the existing the configuration of security association between different Mobile IP entities (home agent, foreign agent, and mobile node). The index objects for this table are the IP address of the entity and the security parameter index (SPI). No object is provided for creation or deletion of new rows in this table via SNMP. Table 16-1 shows the fixed values for objects in the mipSecAssocTable.

Table 16-1 Fixed Security Method for RFC 2006-MIB mipSecAssocTable Objects

Object	Fixed Security Method Value
mipSecAlgorithmType	MD5
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 a home agent or foreign agent service should be started on the interface corresponding to the new row.

  But no object in this table specifies the service (home agent or foreign agent) to be started. Therefore, there should already be one row corresponding to each interface on which the foreign agent or home agent 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 foreign agent. 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. It is not possible to create a new row that corresponds to an interface that is not up.

Send Mobile IP MIB Notifications

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.

To configure the router to send Mobile IP traps or informs to a host, use the following commands in global configuration mode.

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.

Note that Mobile IP notifications need not be enabled on a system to process simple Set or Get SNMP requests.

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

Mobile IP Security Violation Notification Configuration Example

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
```

To enable Simple Network Management Protocol (SNMP) security notifications for Mobile IP, use the **snmp-server enable traps ipmobile** command in global configuration mode. To disable SNMP notifications for Mobile IP, use the **no** form of this command.

SNMP Mobile IP notifications can be sent as traps or inform requests. This command enables both traps and inform requests.

The **snmp-server enable traps ipmobile** command is used in conjunction with the **snmp-server host** command. Use the **snmp-server host** global configuration command to specify which host or hosts receive SNMP notifications. To send SNMP notifications, you must identify at least one **snmp-server host**.

To specify the recipient of a Simple Network Management Protocol (SNMP) notification operation, use the **snmp-server host** command in global configuration mode. To remove the specified host, use the **no** form of this command.

If you enter this command with no keywords, the default is to send all trap types to the host. No informs will be sent to this host.

If no **version** keyword is present, the default is version 1. The **no snmp-server host** command with no keywords will disable traps, but not informs, to the host. In order to disable informs, use the **no snmp-server host informs** command.

Note If the *community-string* is not defined using the **snmp-server community** command prior to using this command, the default form of the **snmp-server community** command will automatically be inserted into the configuration. The password (*community-string*) used for this automatic configuration of the **snmp-server community** will be the same as specified in the **snmp-server host** command. This is the default behavior for Cisco IOS Release 12.0(3) and later releases.

SNMP notifications can be sent as traps or inform requests. Traps are unreliable because the receiver does not send acknowledgments when it receives traps. The sender cannot determine if the traps were received. However, an SNMP entity that receives an inform request acknowledges the message with an SNMP response PDU. If the sender never receives the response, the inform request can be sent again. Thus, informs are more likely to reach their intended destination.

However, informs consume more resources in the agent and in the network. Unlike a trap, which is discarded as soon as it is sent, an inform request must be held in memory until a response is received or the request times out. Also, traps are sent only once, although an inform may be retried several times. The retries increase traffic and contribute to a higher overhead on the network.

If you do not enter an **snmp-server host** global configuration command, no notifications are sent. To configure the router to send SNMP notifications, you must enter at least one **snmp-server host** command. If you enter the command with no keywords, all trap types are enabled for the host.

To enable multiple hosts, you must issue a separate **snmp-server host** command for each host. You can specify multiple notification types in the command for each host.

When multiple **snmp-server host** commands are given for the same host and kind of notification (trap or inform), each succeeding command overwrites the previous command. Only the last **snmp-server host** command will be in effect. For example, if you enter an **snmp-server host inform** command for a host and then enter another **snmp-server host inform** command for the same host, the second command will replace the first.

The **snmp-server host** command is used in conjunction with the **snmp-server enable** global configuration command. Use the **snmp-server enable** command to specify which SNMP notifications are sent globally. For a host to receive most notifications, at least one **snmp-server enable** command and the **snmp-server host** command for that host must be enabled.

However, some notification types cannot be controlled with the **snmp-server enable** command. For example, some notification types are always enabled. Other notification types are enabled by a different command. For example, the linkUpDown notifications are controlled by the **snmp trap link-status** global configuration command. These notification types do not require an **snmp-server enable** command.

Availability of a notification-type option depends on the router type and Cisco IOS software features supported on the router. For example, the **envmon** notification type is available only if the environmental monitor is part of the system. To learn which notification types are available on your system, use the **?** command at the end of the **snmp-server host** command.

If you want to configure a unique SNMP community string for traps, but you want to prevent SNMP polling access with this string, the configuration should include an access list. In the following example, the community string is named comaccess and the access list is numbered 10:

```
snmp-server community comaccess ro 10
snmp-server host 172.20.2.160 comaccess
access-list 10 deny any
```

The following example sends RFC 1157 SNMP traps to the host specified by the name myhost.cisco.com. Other traps are enabled, but only SNMP traps are sent because only **snmp** is specified in the **snmp-server host** command. The community string is defined as comaccess.

```
snmp-server enable traps
snmp-server host myhost.cisco.com comaccess snmp
```

The following example sends the SNMP and Cisco environmental monitor enterprise-specific traps to address 172.30.2.160:

```
snmp-server enable traps snmp
snmp-server enable traps envmon
snmp-server host 172.30.2.160 public snmp envmon
```

The following example enables the router to send all traps to the host myhost.cisco.com using the community string public:

```
snmp-server enable traps
snmp-server host myhost.cisco.com public
```

The following example will not send traps to any host. The BGP traps are enabled for all hosts, but only the ISDN traps are enabled to be sent to a host.

```
snmp-server enable traps bgp
snmp-server host bob public isdn
```

The following example enables the router to send all inform requests to the host myhost.cisco.com using the community string public:

```
snmp-server enable traps
snmp-server host myhost.cisco.com informs version 2c public
```

The following example sends HSRP MIB informs to the host specified by the name myhost.cisco.com. The community string is defined as public.

```
snmp-server enable traps hsrp
snmp-server host myhost.cisco.com informs version 2c public hsrp
```

Workgroup Bridge SNMP Link Traps Example

For a workgroup bridge to generate the SNMP link trap, the following SNMP commands should be entered on the bridge.

```
snmp-server trap-source Dot11Radio0
snmp-server enable traps snmp linkdown linkup
snmp-server host 1.7.35.35 version
```

The IP address of the device receiving the trap should be the static IP address of the loopback interface on the mobile access router instead of the IP address of the Fast Ethernet VLAN interface, because the Fast Ethernet interfaces IP addresses will be dynamic when dynamic host configuration protocol (DHCP) is enabled.

To force the SNMP packets that are typically sent to the Fast Ethernet interface on the mobile access router to be sent to the loopback interface, the following command should also be entered.

arp *1.7.35.35 00ff.ff40.0087* **ARPA BVI1**

where *1.7.35.35 00ff.ff40.0087* is the MAC address of the Fast Ethernet interface on the mobile access router.

To forward the SNMP packet and the non-native VLAN traffic generated by the workgroup bridge associated with a root device in a VLAN environment in infrastructure mode, VLAN trunking should be turned on for the mobile access router Fast Ethernet interface. The **wgb vlan** command should not be configured on the WGB.

You must add a loopback interface with an IP address on workgroup bridge because the SNMP manager on mobile access router needs a static IP address on workgroup bridge side. The following is an example of SNMv3 configuration.

Workgroup Bridge

```
interface Loopback0
 ip address 1.2.3.4 255.255.0.0
 no ip route-cache

snmp-server group labgrp v3 noauth
snmp-server user labusr labgrp v3
snmp-server trap-source Loopback0
snmp-server enable traps snmp linkdown linkup
no snmp-server enable traps tty
snmp-server enable traps disassociate
snmp-server enable traps deauthenticate
snmp-server host 1.7.35.35 version 3 noauth labusr
```

Mobile Access Router

```
snmp-server engineID remote 1.2.3.4 <WGB SNMP engineID>
snmp-server user labusr labgrp remote 1.2.3.4 v3
snmp-server group labgrp v3 noauth
snmp-server manager
snmp-server manager session-timeout <num>
2.authNoPriv:
interface Loopback0
 ip address 1.2.3.4 255.255.0.0
 no ip route-cache

snmp-server group labgrp v3 auth
snmp-server user labusr labgrp v3 auth md5 MD5passwd
snmp-server trap-source Loopback0
snmp-server enable traps snmp linkdown linkup
no snmp-server enable traps tty
snmp-server enable traps disassociate
snmp-server enable traps deauthenticate
snmp-server host 1.7.35.35 version 3 auth labusr
```

Mobile Access Router

```
snmp-server engineID remote 1.2.3.4 <WGB SNMP engineID>
snmp-server user labusr labgrp remote 1.2.3.4 v3 auth md5 MD5passwd
snmp-server group labgrp v3 auth
snmp-server manager
snmp-server manager session-timeout <num>
```

FTP the MIB Files

Follow these steps to obtain each MIB file by using FTP:

Step 1 Use FTP to access the server **ftp.cisco.com**.

Step 2 Log in with the username **anonymous**.

Step 3 Enter your e-mail username when prompted for the password.

Step 4 At the `ftp>` prompt, change directories to **/pub/mibs/v1** or **/pub/mibs/v2**.

Step 5 Use the **get** *MIB_filename* command to obtain a copy of the MIB file.

Note You can also access information about MIBs on the Cisco web site: http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml