

IF-MIBs

This module contains information about MIBs used with interfaces and hardware components. The IF-MIB supports all tables defined in RFC 2863, The Interfaces Group MIB, and the CISCO-IFEXTENSION-MIB. This MIB provides the ability to query the Interfaces MIB objects, and the information returned is restricted to the Virtual Private Network (VPN) routing/forwarding (VRF) instance to which the Simple Network Management Protocol (SNMP) context is mapped. Notification hosts may also be configured with contexts to restrict the notifications that need to be sent to the particular host.

The IF-MIB supports context-aware packet information in VRF environments. VRF environments require that contexts apply to VPNs so that clients can be given selective access to the information stored in the IF-MIB. Clients belonging to a particular VRF can access information about the interface from IF-MIB that belongs only to that VRF. When a client tries to get information from an interface that is associated with a particular context, the client can see the information that belongs to only that context and cannot see information to which it is not entitled.

This document describes the enhancement of the Interfaces Group MIB for subinterfaces and RFC 2233 compliance for Cisco's implementation of the IF-MIB in Cisco IOS software.

- Finding Feature Information, on page 1
- Prerequisites for Using the IF-MIB, on page 2
- Information About the IF-MIB, on page 2
- How to Enable IETF-Compliant Link Traps for SNMP, on page 3
- Example to Enable IETF-Compliant Link Traps for SNMP, on page 4
- How to Configure SNMP and Use the IF-MIB, on page 5
- Additional References, on page 7
- Feature Information for IF-MIBs, on page 8

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.

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

Prerequisites for Using the IF-MIB

To use the Interface Group MIB and Ethernet-like Interface MIB described in this document, you must configure SNMP on your system. It is assumed you will be using Cisco IOS or a network management system (NMS) such as CiscoWorks to monitor the performance of your network. For information on these topics, see the documents listed in the "Related Documents" section or the documentation that came with your network management application.

Information About the IF-MIB

The IF-MIB complies with RFC 2233 and provides SNMP support for subinterfaces. Additionally, you can configure SNMP to use either the existing Cisco implementation of linkUp or linkDown traps or the IF-MIB implementation consistent with IETF standards. Refer to RFC 2233 for information about linkUp and linkDown traps.

You can configure your router to begin using the new RFC 2233 IETF standards-based implementation by using the **snmp-server trap link ietf** command. This command enables notification support for subinterfaces and is disabled by default to allow you to continue using the earlier Cisco implementation of linkUp/linkDown traps if you so choose.

However, please note that when using the earlier Cisco object definitions, an arbitrary value is used for the *locIfReason* object in linkUp/linkDown traps for subinterfaces, which may give you unintended results. This is because the *locIfReason* object is not defined for subinterfaces in the current Cisco implementation, which uses OLD-CISCO-INTERFACES-MIB.my.

If you do not enable this functionality, the link trap varbind list will consist of {ifIndex, ifDescr, ifType, locIfReason}. After you enable this functionality with the **snmp-server trap link ietf** command, the varbind list will consist of {inIndex, ifAdminStatus, ifOperStatus, if Descr, ifType}. The *locIfReason* object will also be conditionally included in this list depending on whether meaningful information can be retrieved for that object. A configured subinterface will generate retrievable information. On non-HWIDB interfaces, there will be no defined value for *locIfReason* , so it will be omitted from the trap message.

Other updates to the IF-MIB module have also been made to comply with RFC2233. These changes include the addition of the ifCounterDiscontinuityTime object, and the addition of basic support for ifTableLastChange. Updated Online Insertion and Removal (OIR) drivers are planned in a future release for full ifTableLastChange support.

Benefits of the IF-MIB

Compliance with RFC 2233

The enhancement to the IF-MIB allows Cisco IOS to support RFC 2233. Prior to this release, Cisco IOS supported only RFC 1573.

linkUp/linkDown Trap Generation for Subinterfaces

The enhancement to the IF-MIB allows linkUp and linkDown SNMP traps for subinterfaces to be generated correctly, while permitting unaffected users to continue using the earlier Cisco implementation.

The Context-Aware IF-MIB

The context-aware IF-MIB provides the ability to query the Interfaces MIB objects and the information returned be restricted to the VRF to which the SNMP context is mapped. Notification hosts may also be configured with contexts to restrict the notifications that need to be sent to the particular host.

In a VPN environment, different interfaces belong to different VRF instances. VRF instances can be uniquely associated with SNMP context. With the context-aware IF-MIB, when SNMP requests that include a specified context mapped to a VRF instance are received, only information related to those interfaces that belong to the VRF associated with the context is obtained.

Retrieve IP Helper Addresses

The IF-MIB enables you to retrieve all IP helper addresses configured on each interface.

How to Enable IETF-Compliant Link Traps for SNMP

Configuration of the IF-MIB is optional on your system and is disabled by default. To configure you need to enable IETF-Compliant Link Traps for SNMP. Perform this task to enable the use of the new object list for SNMP linkUp/linkDown traps, use the following commands, starting in privileged EXEC mode:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server trap link ietf**
4. **end**

DETAILED STEPS

Procedure

	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	**snmp-server trap link ietf** **Example:** `Router(config)# snmp-server trap link ietf`	Enables SNMP traps that are compliant with RFC 2233.

	Command or Action	Purpose
Step 4	**end** **Example:** `Router(config)# end`	Ends the current configuration session and returns you to privileged EXEC mode.

What to do next

Verifying IETF-Compliant Link Traps for SNMP

Use the **more system:running-config** command in privileged EXEC mode to verify that the command is in your running configuration file.

Troubleshooting Tips

To monitor SNMP trap activity in real-time for the purposes of troubleshooting, use the SNMP debug commands, including the **debug snmp packet** command. For documentation of SNMP debug commands, see the Release 12.4 *Cisco IOS Debug Command Reference,* available on Cisco.com at http://www.cisco.com/en/US/docs/ios/debug/command/reference/db_book.html, or on the Cisco Documentation CD-ROM.

Example to Enable IETF-Compliant Link Traps for SNMP

The following example shows the SNMP related output before the IETF-compliant implementation is enabled, a configuration session in which it is enabled, and the changed output after the configuration:

```
Router#
more system:running config
. . .
snmp-server engineID local 00000009000000A1616C2056
snmp-server community public RO
snmp-server community private RW
. . .
Router#
conf term

Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
snmp-server trap link ietf

Router(config)#
end
Router#
 more system:running config
. . .
snmp-server engineID local 00000009000000A1616C2056
snmp-server community public RO
snmp-server community private RW
snmp-server trap link ietf
. . .
```

To enable/disable link traps for a particular interface:

```
7609_supBXL_45(config-if)#snmp trap link-status ?
  permit  Permit the following capability
  <cr>
7609_supBXL_45(config-if)#
```

To enable link up/down traps during switchover:

```
7609_supBXL_45(config)#snmp-server trap link ?
  ietf        Use IETF standard for SNMP traps
  switchover  Enable link up/down traps during switchover
```

How to Configure SNMP and Use the IF-MIB

Configuring the Router to Use SNMP

Before you query IF-MIB feature using SNMP, you must first configure the router to support SNMP.

Note Some of the tasks in this section include examples of the SNMP CLI syntax used to set configuration parameters on the router and to read values from MIB objects on the router. These SNMP CLI syntax examples are taken from a Linux workstation using public domain SNMP tools. The SNMP CLI syntax for your workstation might be different. See the documentation that was provided with your SNMP tools for the correct syntax for your network management workstation.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server community** *string1* **ro**
4. **snmp-server community** *string2* **rw**
5. **end**

DETAILED STEPS

Procedure

	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.

	Command or Action	Purpose
Step 3	**snmp-server community** *string1* **ro** **Example:** `Router(config)# snmp-server community public ro`	Sets up the community access string to permit access to SNMP. • The *string1* argument is a community string that consists of from 1 to 32 alphanumeric characters and functions much like a password, permitting access to the SNMP protocol. Blank spaces are not permitted in the community string. • The **ro** keyword specifies read-only access. SNMP management stations using this string can retrieve MIB objects. **Note** The SNMP community read-only (RO) string for the examples is public. You should use a more complex string for this value in your configuration.
Step 4	**snmp-server community** *string2* **rw** **Example:** `Router(config)# snmp-server community private rw`	Sets up the community access string to permit access to SNMP. • The *string2* argument is a community string that consists of from 1 to 32 alphanumeric characters and functions much like a password, permitting access to the SNMP protocol. Blank spaces are not permitted in the community string. • The **rw** keyword specifies read-write access. SNMP management stations using this string can retrieve and modify MIB objects. **Note** The SNMP community read-write (RW) string for the examples is private. You should use a more complex string for this value in your configuration.
Step 5	**end** **Example:** `Router(config)# end`	Exits the current configuration mode and returns to privileged EXEC mode.

What to Do Next

To implement the IF-MIB, you must configure a tunnel. For information on configuring tunnels, see the "Implementing Tunnels" chapter in this guide.

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 IF-MIBs

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 https://cfnng.cisco.com/. An account on Cisco.com is not required.

Table 1: Feature Information for IF-MIB

Feature Name	Releases	Feature Information
IF-MIB	12.1(2)T 12.0(21)S3 12.3(2)T 12.0(24)S 12.2(2)SXI 12.2(33)SB Cisco IOS Release 3.9S	A router can be configured using the RFC 2233 IETF standards-based implementation. The IF-MIB enables notification support for subinterfaces. The LinkUp/Down traps are generated when a link goes up or down. This feature updates the LinkUp/Down trap information to include ifAdminStatus and ifOperStatus. The IF-MIB supports the IP Helper addresses and enable you to retrieve all IP helper addresses configured on each interface. You have the ability to query the Interfaces MIB objects and the information returned is restricted to the VRF to which the SNMP context is mapped to. Notification hosts may also be configured with contexts to restrict the notifications that need to be sent to a particular host.