IP Tunnel MIBs

Last Updated: December 12, 2011

This module contains information about MIBs used with interfaces and hardware components. The IP Tunnel MIB feature provides a generic MIB for managing all IPv4- and IPv6-related tunnels, as outlined in RFC 4087, IP Tunnel MIB. Tunneling provides a way to encapsulate arbitrary packets inside a transport protocol. A number of tunneling mechanism s specified by Internet Engineering Task Force (IETF) are implemented by Cisco for both IPv4 and IPv6 environments. Various MIBs are available for managing tunnels.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see 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 document.

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 the IP Tunnel MIB

Configure Simple Network Management Protocol (SNMP) on the router on which the IP Tunnel MIB feature is to be used. See the Configuring the Router to Use SNMP, page 4 for more information. For more information on configuring an SNMP server, see the "Configuring SNMP Support " chapter of the Cisco IOS Network Management Configuration Guide.

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Restrictions for the IP Tunnel MIB

The IP Tunnel MIB feature supports only tunnels that can be created using the **interface tunnel** command. The IP Tunnel MIB feature does not support Layer 2 Tunnel Protocol (L2TP), Point-to-Point Tunneling Protocol (PPTP), or Multiprotocol Label Switching (MPLS) tunnels.

Information About the IP Tunnel MIB

Benefits of the IP Tunnel MIB

Improved Quality of Networks

Better IP tunnel instrumentation leads to an improvement in the quality of networks and better service delivery. A better quality network allows service providers to deliver a more reliable service.

Increased Reliability

The IP Tunnel MIB allows users of network management systems to set inventory and receive notification about their IP tunnel activity.

The IP Tunnel MIB supports both IPv4 and IPv6 network layers as defined in RFC 3291, and is used to manage IP tunnels implemented in the Cisco IOS software.

The IP Tunnel MIB supports all tunnel types, as well as tunnel creation and destruction capability.

Interoperability with Devices Other Than Cisco Devices

The IP Tunnel MIB works with key network management systems, including those of third-party vendors.

MIB Objects Supported by the IP Tunnel MIB

The following MIB objects are supported by the IP Tunnel MIB feature. For details regarding use of MIB objects, see RFC 4087, IP Tunnel MIB.

Table 1 Objects Supported by the IP Tunnel MIB

MIB Object	Description
tunnelIfEntry	Contains information on a particular configured tunnel. You can use the **interface tunnel** command to set a value for this object.
tunnelIfEncapsMethod	The encapsulation method used by the tunnel. You can use the **tunnel mode** command to set a value for this object.

MIB Object	Description
tunnelIfHopLimit	Defines the IPv4 time to live (TTL) or IPv6 hop limit to use in the outer IP header. You can use the **tunnel ttl** command to set a value for this object.
tunnelIfSecurity	Used by the tunnel to secure the outer IP header. The value ipsec indicates that IPsec is used between the tunnel endpoints for authentication or encryption, or both.
tunnelIfTOS	Used by the tunnel to set the high 6 bits (the differentiated services codepoint) of the IPv4 type of service (ToS) or IPv6 traffic class in the outer IP header. You can use the **tunnel tos** command to set a value for this object.
tunnelIfFlowLabel	Used to set the IPv6 Flow Label value. This object is supported for tunnels over IPv6. The default value for this object is 0.
tunnelIfAddressType	Shows the type of address in the corresponding tunelIfLocalInetAddress and tunnelIfRemoteInetAddress objects. This object cannot be configured individually through the command-line interface (CLI).
tunnelIfLocalInetAddress	The address of the local endpoint of the tunnel (that is, the source address used in the outer IP header). If the address is unknown, the value is 0.0.0.0 for IPv4 or :: for IPv6. The address type of this object is given by tunnelIfAddressType. You can use the **tunnel source** command to set a value for this object.
tunnelIfRemoteInetAddress	The address of the remote endpoint of the tunnel (that is, the destination address used in the outer IP header). If the address is unknown or the tunnel is not a point-to-point link (for example, a 6-to-4 tunnel), the value is 0.0.0.0 for tunnels over IPv4 or :: for tunnels over IPv6. The address type of this object is given by tunnelIfAddressType. You can use the **tunnel destination** command to set a value for this object.
tunnelIfEncapsLimit	Shows the maximum number of additional encapsulations permitted for packets undergoing encapsulation at this node. A value of -1 indicates that no limit is present (except as result of packet size).
tunnelInetConfigEntry	Contains information on a particular configured tunnel. There will be only one entry for multipoint tunnels and for tunnels that have the remote inet address 0.0.0.0 for IPv4 or :: for IPv6. Only generic routing encapsulation (GRE)/IP and GRE/IPv6 tunnels are created through the MIB.
tunnelInetConfigIfIndex	Shows the value of ifIndex corresponding to the tunnel interface. A value of 0 is not legal in the active state and means that the interface index has not yet been assigned.

MIB Object	Description
tunnelInetConfigStatus	Used to create or delete table entries in the MIB table. You can use the **interface tunnel** to set a value for this object.
tunnelInetConfigStorageType	Indicates the storage type. Only a nonvolatile storage value is supported.

How to Configure SNMP and Use the IP Tunnel MIB

Configuring the Router to Use 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.

Before you can use the IP Tunnel MIB feature, you must first configure the router to support SNMP. Perform this task to enable SNMP on the router.

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
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, page 5

What to Do Next

To implement the IP Tunnel MIB, you must configure a tunnel. For information on configuring tunnels, see the " Implementing Tunnels " chapter in the Cisco IOS Interface and Hardware Component Configuration Guide.

To debug or troubleshoot any issues related to configuring the IP Tunnel MIB through SNMP, use the debug snmp tunnel-mib command. For information on this command see Cisco IOS Interface and Hardware Component Command Reference.

Additional References

Related Documents

Related Topic	Document Title
SNMP commands, complete command syntax, command reference, command history, defaults, defaults, usage guidelines, and examples	*Cisco IOS Network Management Command Reference*
Configuring SNMP Support	*Cisco IOS Network Management Configuration Guide*
Implementing tunnels	*Cisco IOS Interface and Hardware Component Configuration Guide*

Standards

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

MIBs

MIB	MIBs Link
IP Tunnel MIB	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

RFC	Title
RFC 4087	IP Tunnel MIB

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 the Tunnel MIB

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 www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 2 Feature Information for the IP Tunnel MIB

Feature Name	Releases	Feature Information
IP Tunnel MIB	12.2(33)SRB 12.2(1st)SY 12.2(44)SG 12.2(33)SRD 15.0(1)M Cisco IOS XE 3.1.0SG	The IP Tunnel MIB provides a generic MIB for managing all IPv4- and IPv6-related tunnels, as outlined in RFC 4087 IP Tunnel MIB.