



## About This Guide

---

This guide describes the implementation of the Simple Network Management Protocol (SNMP) on Cisco series router configurations for Cisco IOS Release 12.2SB. SNMP provides a set of commands for setting and retrieving the values of operating parameters on the router. Router information is stored in a virtual storage area called a Management Information Base (MIB), which contains many objects that describe router components and provides information about the status of the components.

SNMP provides a set of commands for setting and retrieving the values of operating parameters on the router. Router information is stored in a virtual storage area called a Management Information Base (MIB), which contains many objects that describe router components and provides information about the status of the components. This Preface provides an overview of this guide with the following sections:

- [Revision History, page xi](#)
- [Audience, page xiii](#)
- [Organization, page xiii](#)
- [Document Conventions, page xiv](#)
- [Obtaining Documentation, page xiv](#)
- [Documentation Feedback, page xv](#)
- [Obtaining Technical Assistance, page xvii](#)
- [Obtaining Additional Publications and Information, page xviii](#)

## Revision History

The following Guide Revision History tables record technical changes, additions, and corrections to this document. The table shows the release number and document revision number for the change, the date of the change, and a brief summary of the change.

Changes in MIB support on the Cisco 10000 Series Router occur from Cisco IOS software release to software release.

Cisco IOS Release	Part Number	Publication Date
12.2(31)SB2	OL-4952-04a	December 2006

### Description of Changes

- Updated [MIB Versions for 12.2SB Software Release, page 1](#).

- Updated the [CISCO-ENTITY-ASSET-MIB](#) with ceAssetTag constraints.
- Update [ENTITY-MIB](#)—Added UDI support and table implementation.
- Updated “[Cisco 10000 Series Router MIB Categories](#)” section on page 1.
- Added [CISCO-QINQ-VLAN-MIB](#) feature MIB.
- Added the [CISCO-NETFLOW-MIB](#) which includes SNMP access to important information available in the NetFlow Cache. This is not a replacement for the traditional NetFlow export mechanism, but a method to take a snapshot of the cache register and make it available via SNMP. This functionality is useful for security verification, discovering use of network resources, and identifying top individual contributors to network utilization.
- The [CISCO-CBP-TARGET-MIB](#) contains objects that provide a mapping of targets to which class-based features, such as QoS are applied.  
The CISCO-CBP-TARGET-MIB abstracts the knowledge of the specific types of targets from the class-based policy feature specific MIB definitions.
- Updated Appendix A with CISCO-CBP-TARGET-MIB usage information. See [Appendix 1, “Using CISCO-CBP-TARGET-MIB”](#).
- CISCO-IF-EXTENSION MIB— This MIB provides two tables which provide information about interface packet statistics and interface properties respectively. These objects contain information about the interface or sub interface which is not included in the IF-MIB.
- Interface mapping improvements:
  - Improved existing CISCO-AAA-SESSION-MIB to map sessions to underlying interfaces. See [Using CISCO-AAA-SESSION-MIB, page 47](#).
  - Improved the [IF-MIB](#) infrastructure to turn on PPP session representation and increased memory utilization with various numbers of sessions on a per interface basis.
- Added the [CISCO-IP-URPF-MIB](#) support.
- The [CISCO-TAP2-MIB, page 33](#) has two statistics that are kept for taps:
  - Tap2StreamInterceptedPackets – the number of packets intercepted on this tap. Placed in Column 3 because this statistic can be kept anywhere from column 0 to 4 and 3 is least stressed. The column may change based on other 2.1 feature requirements but will have no impact on the feature. The counter will take a few PXF instructions (6/7) and 4k 32-bit words of XCM.
  - Tap2StreamInterceptDrops – the number of intercepted packet dropped during the intercept process. The inability to IPM\_REPLAY a packet is the only drop that will be counted, therefore this counter must go into column 5. The location and bit-width of this field is uncertain at this time, but it will most likely be 4k 8-bit values in ICM or 32-bit values in XCM based on memory availability.
- [MPLS-VPN-MIB, page 46](#) enhancement implements a new notification, VpnThreshCleared, draft-ietf-ppvnpn-mpls-vpn-mib-06.txt. This notifies the network administrator that the number of routes in a VRF have fallen below the thresholds.
- Enhanced support for the OSPF-MIB to the latest RFC 1850 and adds the latest draft extensions.

Cisco IOS Release	Part Number	Publication Date
12.2(28)SB REL3	OL-4952-03	February 2006

## Description of Changes

- Added Cisco 10000 Series Router MIB categories. See [Cisco 10000 Series Router MIB Categories, page 1](#)
- Added support for the [CISCO-IP-LOCAL-POOL-MIB](#).
- Added [Table 1-1 on page 2](#) which lists the MIB versions that are supported in the 12.2SB REL3 and 12.3(7)XI1 software releases.
- Added support for per-Peer Received Routes in the [BGP4-MIB](#). For detailed information, see New Features in IOS Release 12.2(28)SB at: [http://lbj/push\\_targets1/ucdit/cc/td/doc/product/software/ios122sb/newft/122sb28/index.htm](http://lbj/push_targets1/ucdit/cc/td/doc/product/software/ios122sb/newft/122sb28/index.htm)
- Added enhancements to the [CISCO-FRAME-RELAY-MIB](#). For detailed information, see New Features in IOS Release 12.2(28)SB at: [http://lbj/push\\_targets1/ucdit/cc/td/doc/product/software/ios122/122newft/122t/122t4/ftfrmibe.htm](http://lbj/push_targets1/ucdit/cc/td/doc/product/software/ios122/122newft/122t/122t4/ftfrmibe.htm)

Cisco IOS Release	Part Number	Publication Date
12.3(7)XI1	OL-4952-02	August 2004

## Description of Changes

- Added [CISCO-IP-LOCAL-POOL-MIB, page 25](#).
- Enhanced snmp-server community command. See “[SNMP Usage Guidelines](#)” section on page 4 for details about the snmp-server community command use.

# Audience

This guide is intended for system and network administrators who must configure the router for operation and monitor its performance in the network.

This guide may also be useful for application developers who are developing management applications for the router.

# Organization

This guide contains the following chapters:

- [Chapter 1, “Cisco 10000 Series Router MIB Overview,”](#) provides background information about SNMP and its implementation on the Cisco 10000 series ESR and a history revision table describing what has changed since the last software release.
- [Chapter 2, “Configuring MIB Support,”](#) provides instructions for configuring SNMP management support on the router.
- [Chapter 3, “MIB Specifications,”](#) describes each MIB included in the software image. Each description lists any constraints as to how the MIB is implemented on the router.
- [Chapter 4, “Monitoring Notifications,”](#) describes the SNMP traps and notifications supported by the router.

- [Appendix 1, “Using MIBs,”](#) provides information about how to use SNMP to perform system functions such as physical entity management, alarm monitoring, bulk-file retrieval, and quality of service (QoS).
- Glossary
- Index

## Document Conventions

In this guide, command descriptions use these conventions:

<b>boldface font</b>	Commands, user entry, and keywords appear in <b>bold</b> .
<i>italic font</i>	Arguments for which you supply values and new terms appear in <i>italics</i> .
[ ]	Elements in square brackets are optional.
{ }	Elements in braces are required.
{ x   y   z }	Alternative keywords are grouped in braces and separated by vertical bars.

Examples use these conventions:

screen font	Terminal sessions and information the system displays are in <code>screen font</code> .
<b>bold screen font</b>	Information you must enter is in <b>bold screen font</b> .
< >	Nonprinting characters such as passwords are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.

Notes and cautions use these conventions:



### Note

Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the publication.



### Caution

Means reader be careful. In this situation, you might do something that could result in equipment damage or loss of data.

## Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

## Cisco.com

You can access the most current Cisco documentation at this URL:

<http://www.cisco.com/techsupport>

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

[http://www.cisco.com/public/countries\\_languages.shtml](http://www.cisco.com/public/countries_languages.shtml)

## Product Documentation DVD

Cisco documentation and additional literature are available in the Product Documentation DVD package, which may have shipped with your product. The Product Documentation DVD is updated regularly and may be more current than printed documentation.

The Product Documentation DVD is a comprehensive library of technical product documentation on portable media. The DVD enables you to access multiple versions of hardware and software installation, configuration, and command guides for Cisco products and to view technical documentation in HTML. With the DVD, you have access to the same documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .pdf versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD=) from Cisco Marketplace at this URL:

<http://www.cisco.com/go/marketplace/>

## Ordering Documentation

Beginning June 30, 2005, registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

<http://www.cisco.com/go/marketplace/>

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at [tech-doc-store-mkpl@external.cisco.com](mailto:tech-doc-store-mkpl@external.cisco.com) or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

## Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can send comments about Cisco documentation to [bug-doc@cisco.com](mailto:bug-doc@cisco.com).

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems  
Attn: Customer Document Ordering  
170 West Tasman Drive  
San Jose, CA 95134-9883

We appreciate your comments.

## Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

[http://www.cisco.com/en/US/products/products\\_security\\_vulnerability\\_policy.html](http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html)

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

<http://www.cisco.com/go/psirt>

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

[http://www.cisco.com/en/US/products/products\\_psirt\\_rss\\_feed.html](http://www.cisco.com/en/US/products/products_psirt_rss_feed.html)

## Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—[security-alert@cisco.com](mailto:security-alert@cisco.com)

An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- Nonemergencies—[psirt@cisco.com](mailto:psirt@cisco.com)

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532



### Tip

We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.x through 8.x.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page

at this URL:

[http://www.cisco.com/en/US/products/products\\_security\\_vulnerability\\_policy.html](http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html)

The link on this page has the current PGP key ID in use.

---

## Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

## Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

<http://www.cisco.com/techsupport>

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

<http://tools.cisco.com/RPF/register/register.do>



### Note

Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

---

## Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

<http://www.cisco.com/techsupport/servicerequest>

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/techsupport/contacts>

## Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

**Severity 1 (S1)**—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

**Severity 2 (S2)**—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

**Severity 3 (S3)**—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

**Severity 4 (S4)**—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

## Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:  
<http://www.cisco.com/go/marketplace/>
- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

<http://www.ciscopress.com>

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

<http://www.cisco.com/packet>

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

<http://www.cisco.com/go/iqmagazine>

or view the digital edition at this URL:

<http://ciscoiq.texterity.com/ciscoiq/sample/>

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

<http://www.cisco.com/ipj>

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

<http://www.cisco.com/en/US/products/index.html>

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

<http://www.cisco.com/discuss/networking>

- World-class networking training is available from Cisco. You can view current offerings at this URL:

<http://www.cisco.com/en/US/learning/index.html>

