MPLS VPN SNMP Notifications

This document describes the Simple Network Management Protocol (SNMP) agent support in Cisco IOS for Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) event notifications as implemented in the notifications section of the draft *MPLS/BGP Virtual Private Network Management Information Base Using SMIv2* (*draft-ietf-ppvpn-mpls-vpn-mib-03.txt*).

The MPLS VPN technology allows service providers to offer intranet and extranet VPN services that directly connect their customers' remote offices to a public network with the same security and service levels that a private network offers. The Provider-Provisioned VPN (PPVPN)-MPLS-VPN MIB notifications provide SNMP notification for critical MPLS VPN events.

The MPLS VPN SNMP Notifications feature provides the following benefits:

- A standards-based SNMP interface for retrieving information about critical MPLS VPN events.
- The generation and queuing of notifications that call attention to major changes in the operational status of MPLS VPN enabled interfaces; the forwarding of notification messages to a designated NMS for evaluation and action by network administrators.
- Advanced warning when VPN routing tables are approaching or exceed their capacity.
- Warnings about the reception of illegal labels on a VRF enabled interface. Such receptions may indicate misconfiguration or an attempt to violate security.

Prerequisites for MPLS VPN SNMP Notifications

The MPLS VPN SNMP Notifications feature requires the following:

- SNMP is installed and enabled on the label switching routers.
- Multiprotocol Label Switching (MPLS) is enabled on the label switching routers.

- Multiprotocol Border Gateway Protocol (BGP) is enabled on the label switching routers.
- Cisco Express Forwarding is enabled on the label switching routers.

Restrictions for MPLS VPN SNMP Notifications

- The MPLS-VPN-MIB agent is not implemented in this release.
- Configuration of the MIB using the SNMP SET command is not supported in this release.
- The retrieval of MPLS-VPN-MIB objects using SNMP GET is not supported in this release.

Information About MPLS VPN SNMP Notifications

Cisco Implementation of MPLS VPN MIB

SNMP agent code operating with the notifications of the MPLS VPN SNMP Notifications feature enables a standardized, SNMP-based approach to monitoring the MPLS VPN MIB notifications that aid in the management of Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs) in Cisco software.

The MPLS VPN SNMP Notifications feature is based on the IETF draft specification *draft-ietf-ppvpn-mpls-vpn-mib-02.txt*, which includes notification objects that support MPLS VPN notification events. This IETF draft MIB, which undergoes revisions from time to time, is being evolved toward becoming a standard. Accordingly, the Cisco implementation of features of the MPLS VPN MIB is expected to track the evolution of the IETF draft MIB, and may change accordingly.

Some slight differences between the IETF draft MIB and the actual implementation of MPLS VPNs within Cisco software require some minor translations between the MPLS VPN MIB and the internal data structures of Cisco software. These translations are accomplished by means of the SNMP agent code. Also, while running as a low priority process, the SNMP agent provides a management interface to Cisco software. SNMP adds little overhead on the normal functions of the device.

The SNMP objects defined in the MPLS VPN MIB notifications can be viewed by any standard SNMP utility. The network administrator can retrieve information in the MPLS VPN MIB using standard SNMP **get** and **getnext** operations for SNMP v1, v2, and v3.

All MPLS VPN MIB objects are based on the IETF draft MIB; thus, no specific Cisco SNMP application is required to support the functions and operations pertaining to the MPLS VPN SNMP Notifications feature.

This section contains the following information about the Cisco implementation of the MPLS VPN MIB:

Capabilities Supported by MPLS VPN SNMP Notifications

The following functionality is supported in this release for the MPLS VPN SNMP Notifications feature. This feature provides you with the ability to do the following:

- Create and send notification messages that signal changes when critical Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) events occur.
- Enable, disable, and configure notification messages for MPLS VPN events by using extensions to existing SNMP CLI commands.

- Specify the IP address of a network management system (NMS) in the operating environment to which notification messages are sent.
- Write notification configurations into nonvolatile memory.

Notification Generation Events for the MPLS VPN MIB

The following notifications of the MPLS VPN MIB are implemented for this release:

- **mplsVrfIfUp**—Sent to an NMS when an interface comes up and is assigned a VPN routing/forwarding table instance (VRF).
- **mplsVrfIfDown**—Generated and sent to the NMS when a VRF is removed from an interface or the interface transitions from an operationally "up" state to a "down" state.

Note For the mplsVrfIfUp or mplsVrfIfDown notifications to be issued on ATM or Frame Relay subinterfaces, you must configure the **snmp-server traps atm subif** command or the **snmp-server traps frame-relay subif** command on the subinterfaces, respectively.

- **mplsNumVrfRouteMidThreshExceeded**—Generated and sent when the middle (warning) threshold is crossed. You can configure this threshold in the CLI by using the following commands:

```
Router(config)# ip vrf vrf-name
Router(config-vrf)# maximum routes max-thresh
mid-thresh (% of max)
```

This notification is sent to the NMS only at the time the threshold is exceeded. Whenever the number of routes falls below this threshold and exceeds the threshold again, a notification is sent to the NMS. (See the figure below for a comparison of the warning and maximum thresholds.)

- **mplsNumVrfRouteMaxThreshExceeded**—Generated and sent when you attempt to create a route on a VRF that already contains the maximum number of routes as defined by the following CLI commands:

```
Router(config)# ip vrf vrf-name
Router(config-vrf)# maximum routes max-thresh
mid-thresh (% of max)
```

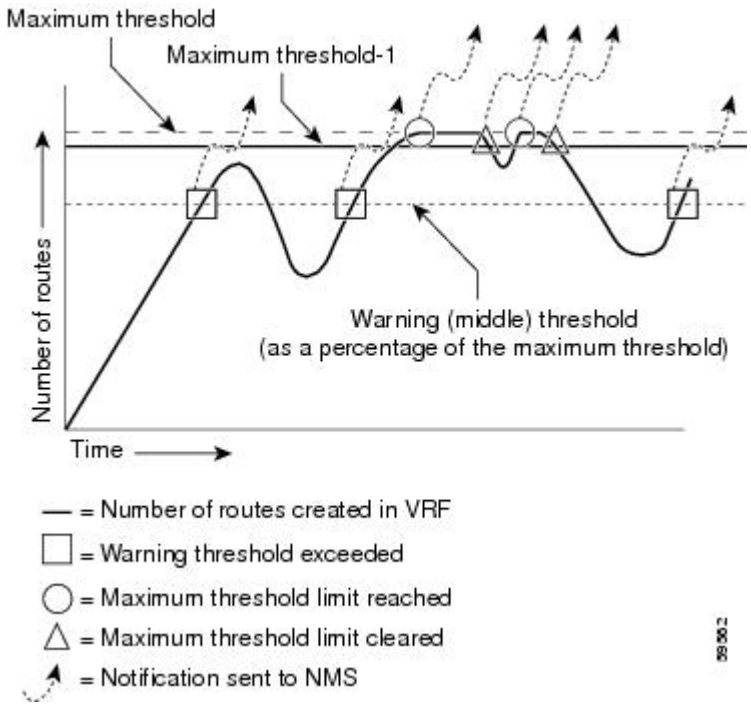
A trap notification is sent to the NMS when you attempt to exceed the maximum threshold. Another notification is not sent until the number of routes falls below the maximum threshold and reaches the maximum threshold again. (See the figure below for an example of how this notification works and for a comparison of the maximum and warning thresholds.)

Note The **maximum routes** command sets the number of routes for a VRF. You *cannot* exceed the number of routes in the VRF that you set with the **maximum routes** *max-thresh* CLI command. Prior to this implementation of the MPLS-VPN-MIB, you were not notified when this threshold (or the warning threshold) was reached.

- **mplsNumVrfSecIllegalLabelThreshExceeded**—Generated and sent when the amount of illegal labels received on a VRF interface exceeds the threshold *mplsVpnVrfSecIllegalLabelRcvThresh*. This threshold

is defined with a value of 0. Therefore, a notification is sent when the first illegal label is received on a VRF. Labels are considered illegal if they are outside of the valid label range, do not have a Label Forwarding Information Base (LFIB) entry, or the table ID of the message does not match the table ID for the label in the LFIB.

Figure 1: Comparison of Warning and Maximum Thresholds



Notification Specification for MPLS-VPN-MIB

In an SNMPv1 notification, each VPN notification has a generic type identifier and an enterprise-specific type identifier for identifying the notification type.

- The generic type for all VPN notifications is “enterpriseSpecific” as this is not one of the generic notification types defined for SNMP.
- The enterprise-specific type is identified as follows:
  - 1 for *mplsVrfIfUp*
  - 2 for *mplsVrfIfDown*
  - 3 for *mplsNumVrfRouteMidThreshExceeded*
  - 4 for *mplsNumVrfRouteMaxThreshExceeded*
  - 5 for *mplsNumVrfSecIllegalLabelThreshExceeded*

In SNMPv2, the notification type is identified by an **SnmpTrapOID** varbind (variable binding consisting of an object identifier (OID) type and value) included within the notification message.

Each notification also contains two additional objects from the MPLS-VPN-MIB. These objects provide additional information about the event, as follows:

- The VRF interface up/down notifications provide additional variables--*mplsVpnInterfaceConfIndex* and *mplsVpnVrfName*-- in the notification. These variables describe the SNMP interface index and the VRF name, respectively.
- The mid and max threshold notifications include the *mplsVpnVrfName* variable (VRF name) as well as the *mplsVpnVrfPerfCurrNumRoutes* variable that indicates the current number of routes within the VRF.
- The illegal label notification includes the *mplsVpnVrfName* variable (VRF name) and the *mplsVpnVrfSecIllegalLabelViolations* variable that maintains the current count of illegal labels on a VPN.

Monitoring the MPLS VPN SNMP Notifications

When MPLS-VPN-MIB notifications are enabled, notification messages relating to specific Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) events within Cisco software are generated and sent to a specified network management system (NMS) in the network. Any utility that supports SNMPv1 or SNMPv2 notifications can receive notification messages.

To monitor MPLS-VPN-MIB notification messages, log in to an NMS that supports a utility that displays SNMP notifications, and start the display utility.

How to Configure the MPLS VPN SNMP Notifications

Configuring an SNMP Community

An SNMP community string defines the relationship between the SNMP manager and the agent. The community string acts like a password to regulate access to the agent on the device.

Perform this task to configure an SNMP community.

SUMMARY STEPS

1. **enable**
2. **show running-config**
3. **configure terminal**
4. **snmp-server community** *string* [**view** *view-name*] [**ro** | **rw**] [*acl-number*]
5. **do copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show running-config** **Example:**	Displays the running configuration to determine if an SNMP agent is already running.

	Command or Action	Purpose
	`Device# show running-config`	If no SNMP information is displayed, continue with the next step. If any SNMP information is displayed, you can modify the information or change it as needed.
Step 3	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 4	**snmp-server community** *string* [**view** *view-name*] [**ro** | **rw**] [*acl-number*] **Example:** `Device(config)# snmp-server community comaccess ro`	Sets up the community access string to permit access to the Simple Network Management Protocol (SNMP). • The *string* argument acts like a password and permits access to the SNMP protocol. • The **view***view-name* keyword and argument specifies the name of a previously defined view. The view defines the objects available to the community. • The **ro** keyword specifies read-only access. Authorized management stations are only able to retrieve MIB objects. • The **rw** keyword specifies read-write access. Authorized management stations are able to both retrieve and modify MIB objects. • The *acl-number* argument is an integer from 1 to 99 that specifies an access list of IP addresses that are allowed to use the community string to gain access to the SNMP agent.
Step 5	**do copy running-config startup-config** **Example:** `Device(config)# do copy running-config startup-config`	Saves the modified configuration to nonvolatile memory (NVRAM) as the startup configuration file. (The **do** command allows you to perform Exec level commands in configuration mode.)

Configuring the Device to Send SNMP Traps

Perform this task to configure the device to send traps to a host.

The **snmp-server host** command specifies which hosts receive traps. The **snmp-server enable traps** command globally enables the trap production mechanism for the specified traps.

Note Although you can set the *community-string* argument using the **snmp-server host** command by itself, we recommend you define this string using the **snmp-server community** command prior to using the **snmp-server host** command.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server host** *host-addr* [**traps** | **informs**] [**version** {**1** | **2c** | **3** [**auth** | **noauth** | **priv**]}] *community-string* [**udp-port** *port*] [*notification-type*]
4. Do one of the following:
   - **snmp-server enable traps atm** [**pvc** | **subif**]
   - **snmp-server enable traps frame-relay** [**subif**]
5. **snmp-server enable traps mpls vpn**
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

Step 3	**snmp-server host** *host-addr* [**traps** | **informs**] [**version** {**1** | **2c** | **3** [**auth** | **noauth** | **priv**]}] *community-string* [**udp-port** *port*] [*notification-type*]
	Example:
	`Device(config)# snmp-server host 172.20.2.160 traps comaccess mpls-vpn`
		Specifies the recipient of an SNMP notification operation.
		• The *host-addr* argument specifies the name or Internet address of the host (the targeted recipient).
		• The **traps** keyword sends SNMP traps to this host. This is the default.
		• The **informs** keyword sends SNMP informs to this host.
		• The **version** keyword specifies the version of the SNMP used to send the traps. Version 3 is the most secure model, as it allows packet encryption with the **priv** keyword. If you use the **version** keyword, you must specify one of the following:
		  • **1**—SNMPv1. This option is not available with informs.
		  • **2c**—SNMPv2C.
		  • **3**—SNMPv3. The following three optional keywords can follow the **version 3** keyword (**auth**, **noauth**, **priv**).
		• The *community-string* argument is a password-like community string sent with the notification operation.

	Command or Action	Purpose
		• The **udp-port** *port* keyword and argument names the UDP port of the host to use. The default is 162. • The *notification-type* argument specifies the type of notification to be sent to the host. If no type is specified, all notifications are sent. MPLS VPN notifications are specified with the **mpls-vpn** keyword.

Step 4	Do one of the following:
	• **snmp-server enable traps atm** [**pvc** | **subif**]
	• **snmp-server enable traps frame-relay** [**subif**]
	Example:
	`Device(config)# snmp-server enable traps atm subif`
	Example:
	`Device(config)# snmp-server enable traps frame-relay subif`
		(For ATM subinterfaces only) Enables the sending of ATM SNMP notifications.
		• The **pvc** keyword enables SNMP ATM permanent virtual circuit (PVC) traps.
		• The **subif** keyword enables SNMP ATM subinterface traps.
		or
		(For Frame Relay subinterfaces only) Enables Frame Relay DLCI link status SNMP notifications.
		• The **subif** keyword enables SNMP Frame Relay subinterface traps.
		Note For mplsVrfIfUp or mplsVrfIfDown notifications to be issued on ATM or Frame Relay subinterfaces, you must configure the appropriate **snmp-server enable traps** command with the **subif** keyword.

Step 5	**snmp-server enable traps mpls vpn** **Example:** `Device(config)# snmp-server enable traps mpls vpn vrf-up vrf-down`	Enables the device to send MPLS VPN SNMP notifications.
Step 6	**end** **Example:** `Device(config)# end`	(Optional) Returns to user EXEC mode.

Configuring Threshold Values for MPLS VPN SNMP Notifications

Perform this task to configure threshold values for MPLS VPN SNMP notifications.

The **mplsNumVrfRouteMidThreshExceeded** notification event is generated and sent when the middle (warning) threshold is crossed. You can configure this threshold in the CLI by using the **maximum routes** command in VRF configuration mode. This notification is sent to the NMS only at the time the threshold is

exceeded. Whenever the number of routes falls below this threshold and exceeds the threshold again, a notification is sent to the NMS.

The **mplsNumVrfRouteMaxThreshExceeded** notification event is generated and sent when you attempt to create a route on a VRF that already contains the maximum number of routes as defined by the **maximum routes** command in VRF configuration mode. A trap notification is sent to the NMS when you attempt to exceed the maximum threshold. Another notification is not sent until the number of routes falls below the maximum threshold and reaches the maximum threshold again.

(See the figure above for an example of how this notification works and for a comparison of the maximum and warning thresholds.)

Note The **maximum routes** command sets the number of routes for a VRF. You *cannot* exceed the number of routes in the VRF that you set with the **maximum routes** *max-thresh* CLI command. Prior to this implementation of the MPLS-VPN-MIB, you were not notified when this threshold (or the warning threshold) was reached.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip vrf** *vrf-name*
4. **maximum routes** *limit* {*warn-threshold* | **warning-only**}
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ip vrf** *vrf-name* **Example:** `Device(config)# ip vrf vpn1`	Configures a VRF routing table. • The *vrf-name* argument specifies the name assigned to a VRF.
Step 4	**maximum routes** *limit* {*warn-threshold*	**warning-only**} **Example:** `Device(config-vrf)# maximum routes 10000 80`	Limits the maximum number of routes in a VRF to prevent a PE device from importing too many routes. • The *limit* argument specifies the maximum number of routes allowed in a VRF. You may select from 1 to 4,294,967,295 routes to be allowed in a VRF.

	Command or Action	Purpose
		• The *warn-threshold* argument specifies when the threshold limit is reached and routes are rejected. The threshold limit is a percentage of the *limit* specified, from 1 to 100 percent. • The **warning-only** keyword specifies that a SYSLOG error message is issued when the maximum number of routes allowed for a VRF exceeds the threshold. However, additional routes are still allowed.
Step 5	**end** **Example:** `Device(config-vrf)# end`	(Optional) Returns to privileged EXEC mode.

Configuration Examples for MPLS VPN SNMP Notifications

Example: Configuring the Community

The following example shows enabling a simple SNMP community group. This configuration permits any SNMP client to access all MPLS-VPN-MIB objects with read-only access using the community string comaccess.

```
Device# configure terminal
Device(config)# snmp-server community comaccess ro
```

Verify that the SNMP master agent is enabled for the MPLS VPN SNMP Notifications feature:

```
Device# show running-config | include snmp-server
Building configuration...
....
snmp-server community comaccess RO
....
```

Note If you do not see any "snmp-server" statements, SNMP has not been enabled on the device.

Example: Configuring the Device to Send SNMP Traps

The following example shows you how to enable the device to send MPLS VPN notifications to host 172.20.2.160 using the comaccess community string if a VRF transitions from a down state to an up state or from an up state to a down state.

```
Device# configure terminal
Device(config)# snmp-server host 172.20.2.160 traps comaccess mpls-vpn
Device(config)# snmp-server enable traps mpls vpn vrf-up vrf-down
```

Example: Configuring Threshold Values for MPLS VPN SNMP Notifications

The following example shows how to set a maximum threshold or 10000 routes and a warning threshold that is 80 percent of the maximum threshold for a VRF named vpn1 on a device:

```
Device(config)# ip vrf vpn1
Device(config)# maximum routes 10000 80
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
MPLS commands	Cisco IOS Multiprotocol Label Switching Command Reference
MPLS Virtual Private Network (VPN) configuration tasks	"MPLS Virtual Private Networks" module in the *MPLS Layer 3 VPNs Configuration Guide*

MIBs

MIBs	MIBs Link
MPLS/BGP Virtual Private Network Management Information Base Using SMIv2 (*draft-ietf-ppvpn-mpls-vpn-mib-03.txt*) MPLS-VPN-MIB.my	To obtain lists of supported MIBs by platform and Cisco software 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

RFCs	Title
RFC 2233	*The Interfaces Group MIB using SMIv2*

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 MPLS VPN SNMP Notifications

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 1: Feature Information for MPLS VPN SNMP Notifications

Feature Name	Releases	Feature Information
MPLS VPN SNMP Notifications	12.0(21)ST 12.0(22)S 12.2(13)T	The MPLS VPN SNMP Notifications feature provides Simple Network Management Protocol (SNMP) agent support in Cisco software for Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) event notifications. In Cisco IOS Release 12.0(21)ST, this feature was introduced. In Cisco IOS Release 12.0(22)S, this feature was integrated. In Cisco IOS Release 12.2(13)T, this feature was integrated. Supported platforms: • Cisco IOS 12.0 S and ST Releases: Cisco 7500 series, Cisco 12000 series. • Cisco IOS 12.2 T Releases: Cisco 3620, Cisco 3640, Cisco 7200 series, Cisco 7500 series, Cisco MGX 8850-RPM. **Note** In Cisco IOS Releases 12.0(21)ST and 12.0(22)S, the PPVPN MPLS-VPN-MIB notifications are described in the *MPLS VPN--SNMP MIB Support* feature module. The following commands were introduced or modified: **snmp-server enable traps mpls vpn**, **snmp-server host**.

Glossary

ASN.1—Abstract Syntax Notation One. OSI language for describing data types independent of particular computer structures and representation techniques. Described by ISO International Standard 8824.

BGP—Border Gateway Protocol. The exterior Border Gateway Protocol used to exchange routing information between routers in separate autonomous systems. BGP uses Transmission Control Protocol (TCP). Because TCP is a reliable protocol, BGP does not experience problems with dropped or fragmented data packets.

CEF—Cisco Express Forwarding. An advanced Layer 3 IP switching technology. CEF optimizes network performance and scalability for networks with large and dynamic traffic patterns.

CE device—customer edge router. A router on the border between a VPN provider and a VPN customer that belongs to the customer.

community—In SNMP, a logical group of managed devices and NMSs in the same administrative domain.

community name—*See* community string.

community string—Text string that acts as a password and is used to authenticate messages sent between a managed station and a router containing an SNMP agent. The community string is sent in every packet between the manager and the client. Also called a community name.

IETF—Internet Engineering Task Force. Task force consisting of over 80 working groups responsible for developing Internet standards. The IETF operates under the auspices of ISOC. *See also* ISOC.

informs—A type of notification message that is more reliable than a conventional trap notification message, because the informs message notification requires acknowledgment, and a trap notification does not.

ISOC—Internet Society. International nonprofit organization, founded in 1992, that coordinates the evolution and use of the Internet. In addition, ISOC delegates authority to other groups related to the Internet, such as the IAB. ISOC is headquartered in Reston, Virginia (United States).

label—A short, fixed-length data construct that tells switching nodes how to forward data (packets or cells).

label distribution protocol—*See* LDP.

label forwarding information base—*See* LFIB.

label switch router—*See* LSR.

LDP —label distribution protocol. A standard protocol between MPLS-enabled routers that is used for the negotiation of the labels (addresses) used to forward packets.

LFIB —label forwarding information base. In the Cisco Label Switching system, the data structure for storing information about incoming and outgoing tags (labels) and associated equivalent packets suitable for labeling.

LSR —label switch router. A device that forwards MPLS packets based on the value of a fixed-length label encapsulated in each packet.

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

MPLS —Multiprotocol Label Switching. A method for forwarding packets (frames) through a network. It enables routers at the edge of a network to apply labels to packets (frames). ATM switches or existing routers in the network core can switch packets according to the labels with minimal lookup overhead.

MPLS interface—An interface on which MPLS traffic is enabled.

MPLS VPN—Multiprotocol Label Switching Virtual Private Network. Using MPLS VPNs in a Cisco network provide the capability to deploy and administer scalable Layer 3 VPN backbone services including applications, data hosting network commerce, and telephony services, to business customers. A VPN is a secure IP-based network that shares resources on one or more physical networks. A VPN contains geographically dispersed sites that can communicate securely over a shared backbone.

For an MPLS VPN Solution, an MPLS VPN is a set of PEs that are connected by means of a common "backbone" network to supply private IP interconnectivity between two or more customer sites for a given customer. Each VPN has a set of provisioning templates and policies and can span multiple provider administrative domains (PADs).

Multiprotocol label Switching—*See* MPLS.

notification —A message sent by an SNMP agent to a network management station, console, or terminal to indicate that a significant event within Cisco software has occurred. *See also* trap.

NMS —network management system. A powerful, well-equipped computer (typically an engineering workstation) that is used by a network administrator to communicate with other devices in the network. An NMS is typically used to manage network resources, gather statistics, and perform a variety of network administration and configuration tasks.

PE device—provider edge router. A router on the border between a VPN provider and a VPN customer that belongs to the provider.

PPVPN —Provider-Provisioned VPN. The name of the IETF working group that is developing the PPVPN-MPLS-VPN MIB (MPLS-VPN-MIB).

QoS —quality of service. Measure of performance for a transmission system that reflects its transmission quality and service availability.

RSVP —Resource Reservation Protocol. Protocol for reserving network resources to provide Quality of Service guarantees to application flows.

Simple Network Management Protocol—*See* SNMP.

SNMP —Simple Network Management Protocol. Network 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. See *also* SNMP2.

SNMP2 —SNMP Version 2. Version 2 of the popular network management protocol. SNMP2 supports centralized as well as distributed network management strategies, and includes improvements in the SMI, protocol operations, management architecture, and security. *See also* SNMP.

traffic engineering—The techniques and processes used to cause routed traffic to travel through the network on a path other than the one that would have been chosen if standard routing methods had been used.

trap —A message sent by an SNMP agent to a network management station, console, or terminal, indicating that a significant event occurred. Traps (notifications) are less reliable than inform requests, because the receiver does not send an acknowledgment when it receives a trap. The sender cannot determine if the trap was received. *See also* notification.

VPN —Virtual Private Network. A group of sites that, as the result of a set of administrative policies, are able to communicate with each other over a shared backbone network. *See* MPLS VPN.

VRF —VPN routing/forwarding instance. A VRF consists of an IP routing table, a derived forwarding table, a set of interfaces that use the forwarding table, and a set of rules and routing protocols that determine what

goes into the forwarding table. In general, a VRF includes the routing information that defines a customer VPN site that is attached to a PE device.