NORTEL NETWORKS

Preside Multiservice Data Manager

Service Provisioning for IP VPN Global Update

User Guide

241-6001-601

Preside Multiservice Data Manager

Service Provisioning for IP VPN Global Update

User Guide

Publication: 241-6001-601
Document status: Standard
Document version: 14.3RSUP
Document date: December 2003

Printed in Canada

Publication history

December 2003

14.3RSUP Standard
Commercial availability

Contents

About this document **11**
Who should read this document and why 11
What you need to know 12
How this document is organized 12
What's new in this document 12
Text conventions 12
Related documents 14

Chapter 1
IP VPN global update tool overview **15**
Overview 15
Route Reflector 16
Auto Discovery 17
Architecture 18
IP VPN global server 18
IP VPN database 18
End-to-end server 20
IP VPN global update CLI 20
IP VPN global update GUI 20
Limitations and restrictions 21

Chapter 2
Configuring the servers and starting the tool **23**
Server options 23
Configuring the servers 24
Configuring the end-to-end server 24
Configuring the IP VPN global server 25

Changing the server port number and host name 26
Configuring and accessing the server host 27
Starting the IP VPN global update tool (GUI) 28
Preside MDM window 28
Nodal Provisioning main window 28
Network Viewer Start Tool menu 28
Starting the IP VPN global update tool (CLI) 31

Chapter 3
Installing the IP VPN global update tool 33
System requirements 33
Installing the IP VPN global update tool software 34
Installing and configuring MDM software 34
Updating the license 34

Chapter 4
IP VPN global update tool GUI 37
IP VPN global update tool main window 37
Menu bar 40
File menu 40
Edit menu 40
Selected menu 40
Tools menu 42
Help menu 43
Hierarchy tree panel 43
Details panel 43
IP VPN global update tool GUI dialogs 55
Options dialog 56
Confirm Provisioning Options dialog 59
Include VR dialog 62
CoS Policy Group dialog 63
Add New CoS Policy dialog 66
Modify CoS Policy dialog 69
New Flow Classification dialog 71
Modify Flow Classification dialog 73
Exclude VR dialog 75

Error and Message dialogs 76
Progress dialogs 77

Chapter 5
Using the IP VPN global update tool GUI 79
Selecting a device view for provisioning, and saving provisioning data 79
Service provider selected menu procedures 80
Adding a new customer 80
Customer selected menu procedures 81
Removing a customer 81
Adding a new VPN to a customer 82
VPN selected menu procedures 83
Adding a VR to a VPN 83
Removing a VPN 85
Applying IP CoS to a VPN 86
VR selected menu procedures 90
Excluding or deleting a VR from an existing VPN 90
Creating a new customer VPN 91

Chapter 6
Using the IP VPN global update tool CLI 93
Creating a VPN 93
Deleting a VPN 97
Adding a VR to a VPN 97
Excluding a VR from a VPN 98
Deleting a VR 99
Adding a policy group to a VR in a VPN 99
Deleting a policy group from a VR in a VPN 101
Configuring a tosMask attribute on a VR 102
Updating a password 103

Chapter 7
Commands 105
help 105
createvpn 106
createvr 107

includevr 108
excludevr 111
deletevr 113
deletevpn 115
settosmask 116
settosmarking 118
addpolicy 120
deletepolicy 122
listvpn 124
listcustomer 125
updatepasswd 125

Index **127**

About this document

This document explains how to use the Internet Protocol (IP) virtual private network (VPN) global update tool.

ATTENTION	If you have upgraded to Preside MDM Release 14.3, use the IP VPN Service Provisioning tool to configure RFC 2764 VPNs with auto-discovery enabled. See 241-6001-616 *Preside MDM IP VPN Service Configuration User Guide*. Further information can be found the the 14.3 Release Supplement.

The following topics are discussed in this section:

- "Who should read this document and why" (page 11)
- "What you need to know" (page 12)
- "How this document is organized" (page 12)
- "What's new in this document" (page 12)
- "Text conventions" (page 12)
- "Related documents" (page 14)

Who should read this document and why

This guide is intended for personnel who provision IP VPNs on Passport 7000 15000 and 20000 devices.

What you need to know

This document assumes that you have knowledge of the Nortel Networks Preside Multiservice Data Manager (MDM) and have an understanding of the Passport product.

How this document is organized

The information in this document is organized as follows:

- "Installing the IP VPN global update tool" (page 33) describes the IP VPN global update tool, and its software components.
- "Installing the IP VPN global update tool" (page 33) describes the software required for the IP VPN global update tool and how to install it.
- "Configuring the servers" (page 24) describes how to configure the end-to-end server and the IP VPN global server, as well as system requirements and how to launch the IP VPN global update tool.
- "IP VPN global update tool GUI" (page 37) describes the main window and dialogs of the IP VPN global update tool user interface.
- "Using the IP VPN global update tool GUI" (page 79) contains the procedures you can perform with the IP VPN Global Update tool graphical user interface.
- "Commands" (page 105) lists the available commands and their parameters.
- "Using the IP VPN global update tool CLI" (page 93) contains procedures you can perform with the IP global update tool.

What's new in this document

There are no changes in this document for this release.

Text conventions

This document uses the following text conventions:

- `nonproportional spaced plain type`

  Nonproportional spaced plain type represents system generated text or text that appears on your screen.

- **`nonproportional spaced bold type`**

  Nonproportional spaced bold type represents words that you should type or that you should select on the screen.

- *italics*

  Statements that appear in italics in a procedure explain the results of a particular step and appear immediately following the step.

  Words that appear in italics in text are for naming.

- `[optional_parameter]`

  Words in square brackets represent optional parameters. The command can be entered with or without the words in the square brackets.

- `<general_term>`

  Words in angle brackets represent variables which are to be replaced with specific values.

- UPPERCASE,lowercase

  In MDM, uppercase and lowercase letters that appear in UNIX commands and parameters must be matched exactly. The system matches upper and lowercase characters differently.

- |

  This symbol separates items from which you may select one; for example, ON|OFF indicates that you may specify ON or OFF. If you do not make a choice, a default ON is assumed.

- ...

  Three dots in a command indicate that the parameter may be repeated more than once in succession.

The term absolute pathname refers to the full specification of a path starting from the root directory. Absolute pathnames always begin with the slash (/) symbol. A relative pathname takes the current directory as its starting point, and starts with any alphanumeric character (other than /).

Related documents

See the following documents for related information:

- 241-6001-303 *Preside MDM Administrator Guide*
- 241-6001-310 *Preside MDM Server Reference Guide*
- 241-6001-610 *Preside MDM Nodal Provisioning User Guide*
- 241-6001-611 *Preside MDM Nodal and Service Provisioning Reference Guide*

Chapter 1
IP VPN global update tool overview

ATTENTION	If you have upgraded to Preside MDM Release 14.3, use the IP VPN Service Provisioning tool to configure RFC 2764 VPNs with auto-discovery enabled. See 241-6001-616 *Preside MDM IP VPN Service Configuration User Guide*. Further information can be found the the 14.3 Release Supplement.

For an overview of the Internet Protocol (IP) Virtual Private Network (VPN) global update tool, see the following sections:

- "Overview" (page 15)
- "Architecture" (page 18)
- "Limitations and restrictions" (page 21)

Overview

The IP VPN global update tool allows you to set up and perform global updating of a customer IP VPN on Passport 7000, 15000, and 20000 devices through either a graphical user interface (GUI) or a command line interface (CLI). The tool can support a maximum of 1000 VRs per VPN.

The tool allows you to perform the following tasks:

- create a virtual router (VR) component
- include a VR in a VPN
- exclude a VR from a VPN

- set up a border gateway protocol (BGP) between VRs in a VPN
- define IP class of service (CoS) policy groups for the VRs in a VPN
- list operational VPN information

The IP VPN global update tool also provides the following functionality:

- route reflector
- auto discovery

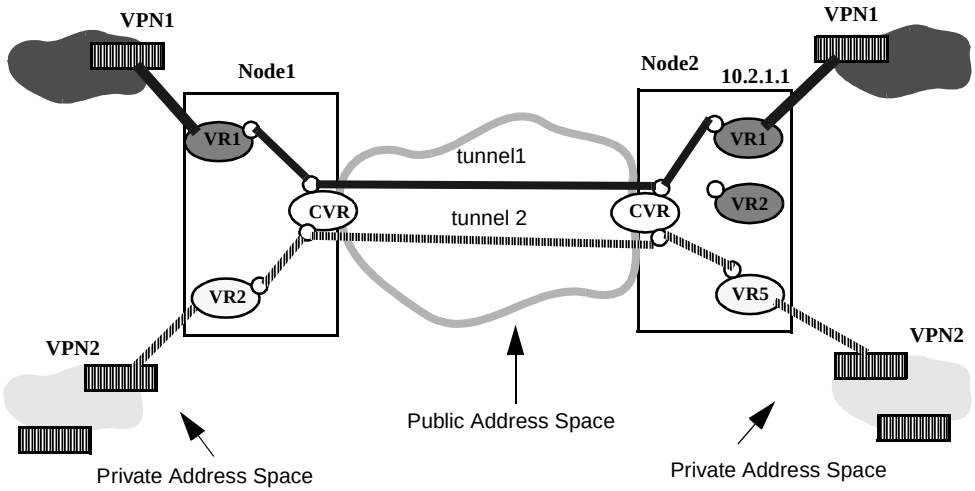
Route Reflector

The IP VPN Global Update Tool uses route reflector functionality which allows you to specify which VRs in the VPN will be route reflectors. If you configure a VR as a route reflector, the VR sends information to other VRs in the VPN. This reduces network traffic, since only the VRs configured as route reflectors send information to the other VRs.

IP tunneling allows you to connect two physically separated networks that share the same (private) address space through an IP network with a different (public) address space. When you include or exclude a VR, the tunnels and ARP tables are updated. Address resolution protocol (ARP) tables map private IP addresses to public IP addresses.

The figure “IP tunneling example” (page 17) shows a sample configuration with two VPNs.

Figure 1
IP tunneling example



CVR=carrier virtual router

Auto Discovery

The IP VPN global update tool provides the option to run the tool in auto discovery mode. Auto discovery mode allows the Passport Virtual Routers (VRs) to dynamically exchange the IP VPN topology information across VPN sites every time a customer VR is added or deleted.

When you select the auto discovery mode, you reduce the amount of provisioning required when adding or deleting new VPN sites by eliminating the following tasks:

- provisioning a static ARP entry for each remote IP tunnel endpoint defined on the customer VR
- specifying the destination address while provisioning a PTMP IP tunnel on the customer VR
- provisioning local IBGP peers on the customer VR

- visiting all remote customer VRs provisioned on remote Passports to update their corresponding IBGP peers, PTMP IP tunnels and ARP entries with information related to the newly provisioned customer VR

Architecture

The IP VPN global update tool consists of the following software components:

- IP VPN global server
- IP VPN database
- End-to-end server
- IP VPN global update CLI
- IP VPN global update GUI

IP VPN global server

The IP VPN global server provides the main functionality of the IP VPN global update tool. The global server also communicates with the IP VPN database to store, update, and list customer VPN-related information. The IP VPN global server uses the end-to-end server to communicate with Passport switches and to send provisioning commands to them. The global server also accesses the IP VPN global database to store and list VPN information.

IP VPN database

The IP VPN database groups and stores VPN-related information. The IP VPN global update tool collects data for a specific VPN when performing IP VPN global updating. The database is located in /opt/MagellanNMS/data/vpn/db.

The database lists all VRs in each VPN. The database consists of one global table containing a list of all VPNs. The VPN list includes the customer name and ID, and the VPN name and ID. The customer name and VPN name uniquely identifies a VPN.

The table “VPN list fields” (page 19) describes the fields in the VPN list.

Table 1
VPN list fields

Field	Description
CUSTOMER	VPN customer name
CUSTOMER_ID	unique customer identifier
VPN	the name of the VPN
VPN_ID	unique VPN identifier
AS	autonomous system ID for BGP routing
USERID	the default userID which you can use to log in to all Passports in the VPN
PASSWD	the password for the userID
AUTODISCOVERY	indicates that the tool is running in autodiscovery mode

The database also provides a VR table for each VPN. The VR table stores the following information:

- the VRs in the specific VPN
- the public and private IP address
- the network mask
- the Passport on which a VR exists

The table describes the fields in the VR table.

Table 2
VR table fields

Field	Description
VR	name of the virtual router in the VPN
PP	name of the Passport in which the VR exists
(Sheet 1 of 2)	

Table 2
VR table fields (continued)

Field	Description
CARRIER_VR	the carrier VR to which the customer VR is mapped
PRIVATE_IP	IP address for the logical interface on the tunnel IP port of the VR
PRIVATE_NETMASK	network mask for the private IP address
PUBLIC_IP	IP address of the logical interface on the virtual media IP port of the carrier VR
PUBLIC_NETMASK	the network mask of the public IP address
ROUTEREFLECTOR	indicates whether a VR acts as a route reflector in the VPN
USERID	the userID when logging into the Passport where the VR exists
PASSWD	the password for the userID
TOPOLOGY	indicates whether the VR is a hub or spoke

(Sheet 2 of 2)

End-to-end server

The end-to-end server acts as an intermediary between the IP VPN global update server and the Preside Multiservice Data Manager (MDM) command console functional process (CMCFUN) server. The CMCFUN server forwards operator commands to Passport devices for execution.

IP VPN global update CLI

IP VPN global update CLI lets you perform global updates by executing commands.

IP VPN global update GUI

The IP VPN global update GUI lets you perform global updates using a graphical user interface. The IP VPN GUI uses the same interface to communicate with the IP VPN server as that which is used by the CLI.

Limitations and restrictions

The following limitations and restrictions apply to the IP VPN global update tool:

- The IP VPN global update server is supported on the Solaris platform only.
- The IP VPN global update CLI client is supported on the Solaris platform only.
- Only Passport 7000 and Passport 15000 products are supported.
- There is no support for database resynchronization.
- The IP VPN global update tool is limited to single user access.
- There is no support for access port or carrier provisioning.

Chapter 2
Configuring the servers and starting the tool

ATTENTION	If you have upgraded to Preside MDM Release 14.3, use the IP VPN Service Provisioning tool to configure RFC 2764 VPNs with auto-discovery enabled. See 241-6001-616 *Preside MDM IP VPN Service Configuration User Guide*. Further information can be found the the 14.3 Release Supplement.

For configuration and start-up instructions for the IP VPN global update tool, see the following sections:

- "Server options" (page 23)
- "Configuring the servers" (page 24)
- "Starting the IP VPN global update tool (GUI)" (page 28)
- "Starting the IP VPN global update tool (CLI)" (page 31)

Server options

Note: To run the IP VPN global server, the end-to-end server must be running. The end-to-end server checks for a valid license key. See "Updating the license" (page 34).

The following IP VPN global server options apply to the IP VPN global update tool:

- -h to obtain help on a command.
- -log to turn logging off or on. The log files are located in /opt/MagellanNMS/data/vpn/log.

- -p to specify a port (by default, the port is 6800).
- -db to specify an alternate path for the database. By default, the database is located in /opt/MagellanNMS/data/vpn/db. The file name of the database is the customer_id number.

Configuring the servers

Before using the IP VPN global update tool, you need to do some or all of the following configuration tasks:

- "Configuring the end-to-end server" (page 24)
- "Configuring the IP VPN global server" (page 25)
- "Changing the server port number and host name" (page 26)
- "Configuring and accessing the server host" (page 27)

Configuring the end-to-end server

Note: Only perform this procedure if the end-to-end server is not configured. If the server is configured, perform the procedure "Configuring the IP VPN global server" (page 25).

You need to use the Server Manager (SVM) Administration tool to edit the entry for the IP VPN end-to-end server. For more information on the end-to-end server, see 241-6001-310 *Preside MDM Server Reference Guide*. For information on the Server Manager Administration (SVM) tool, see 241-6001-303 *Preside MDM Administrator Guide*.

1 While logged on as root, in the Preside MDM window, select System -> Administration -> Server Administration.

The Server Manager Administration tool window opens.

2 From the Security menu, select Enable Editing.

The SVM Enter Edit Password dialog opens and prompts for a password.

3 If required, type a valid password and click OK.

The Server Manager Edit Server dialog opens.

4 From the Edit menu, select the New command.

5 In the Descriptive name field, type the following information:

`end-to-end server`

6 In the Startup command field, type the following information:

`/opt/MagellanNMS/bin/eteserver [-h] [-p <portno>] [-t <timeout>]`

where:

{-h} displays help

[-p <portno>] specifies the TCP port number for monitoring incoming requests. The default value is 6600.

[-t <timeout>] specifies the sleep timeout seconds before attempting connection to servers.

Note: The port number must not be used by any other process.

7 Enable the Automatic startup at reboot time option.

8 Click Save and Start.

The data you entered is stored and the server is started.

9 From the File menu, choose Refresh Server list.

An updated server list is displayed, including the end-to-end server.

Configuring the IP VPN global server

You need to use the Preside Multiservice Data Manager (MDM) Server Manager (SVM) Administration tool to edit the entry for the IP VPN global server. For more information on the IP VPN global server, see 241-6001-310 *Preside MDM Server Reference Guide*.

1 While logged on as root, on the Preside MDM window, select System -> Administration -> Server Administration.

The Server Manager Administration Tool window opens.

2 From the Security menu, select Enable Editing.

The SVM Enter Edit Password dialog opens and prompts for a password.

3 If required, type a valid password and click OK.

The Server Manager Edit Server dialog opens.

4 From the Edit menu, select the New command.

5 In the Descriptive name field, type the following information:

`ipvpn server`

6 In the Startup command field, type the following information:

`/opt/MagellanNMS/bin/ipvpnserver [-p <portno>] [-log]`

where:

[-p <portno>] specifies the TCP port number for monitoring incoming requests. The default value is 6800.

[-log] specifies whether you want logging turned on. If you do not enter this option, logging is not turned on.

Note: The port number must not be used by any other process.

7 Enable the Automatic startup at reboot time option.

8 Click Save and Start.

The data you entered is stored and the server is started.

9 From the File menu, choose Refresh Server list.

An updated server list is displayed, including the ipvpn server.

Changing the server port number and host name

If your setup runs the IP VPN global server on a port other than the default, you need to update the client resource file for the provisioning tool and reconfigure the server.

1 While logged on as root, edit the resource file:

/opt/MagellanNMS/cfg/IP_VPN_Server.txt

2 Set the host parameter:

host = <hostname>|<ipaddress>

where:

<hostname> is the host name.

<ipaddress> is the address of the host server.

3 To change the server port number from the default value of 6800, set the port parameter to the appropriate port number:

port = <portno>

where:

<portno> is the TCP port number.

4 Go to the Preside MDM Server Manager Administration tool and edit the server port number option. See “Configuring the IP VPN global server” (page 25).

5 Restart the IP VPN global server.

Configuring and accessing the server host

By default, the local host is used as the server host. If you are running the client on a different host than the server, you need to update the resource and host files.

Configuring the server host

1 While logged on as root, edit the resource file:

/opt/MagellanNMS/cfg/IP_VPN_Client.txt

2 Set the host parameter:

host = <hostname>|<ipaddress>

where:

<hostname> is the host name.

<ipaddress> is the address of the host server.

3 To change the server port number from the default value of 6800, set the port parameter to the appropriate port number:

port = <portno>

where:

<portno> is the TCP port number.

4 Go to the Preside MDM Server Manager Administration tool and edit the server port number option. See “Configuring the IP VPN global server” (page 25).

Accessing the server host

1 While logged on as root, display the contents of the hosts file:

more /etc/hosts

2 Check that the file contains an entry with the IP address and host name of the server.

3 If the entry is not listed, open an edit view of the resource file and add the IP address and host name on a new line:

<ipaddress> <hostname>

Starting the IP VPN global update tool (GUI)

You can start the IP VPN global update tool from the following points in Preside Multiservice Data Manager (MDM):

- "Preside MDM window" (page 28)
- "Nodal Provisioning main window" (page 28)
- "Network Viewer Start Tool menu" (page 28)

Preside MDM window

1. Start the Preside Multiservice Data Manager (MDM).
2. In the Preside MDM window, select Configuration -> Passport Devices -> Service Provisioning -> IP VPN Global Update.

   The Service Provisioning - IP VPN Global Update tool main window opens.

Nodal Provisioning main window

1. Start the Preside Multiservice Data Manager (MDM).
2. Launch the Nodal Provisioning tool. See in 241-6001-610 *Preside MDM Nodal Provisioning User Guide*.
3. In the menu bar of the Nodal Provisioning tool main window, select External Tools -> Service Provisioning -> IP VPN Global Update.

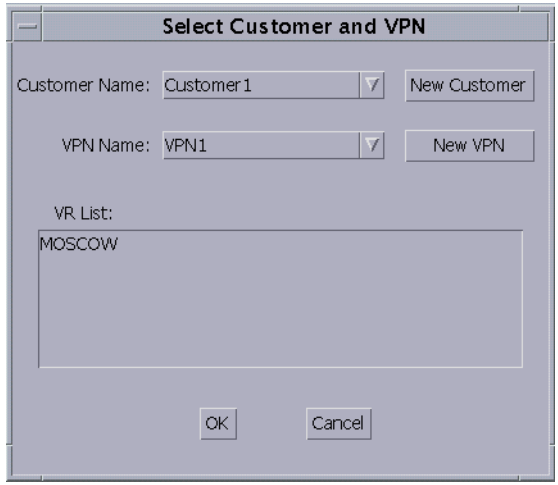
Network Viewer Start Tool menu

1. Launch the Preside Multiservice Data Manager (MDM).
2. In the MDM window, select -> Fault -> Network Viewer.

   The Network Viewer window opens.
3. In the Network Viewer, select the nodes required to provision the IP VPN service by doing one of the following:
   - click on the background of the Network Viewer window, drag the mouse and release it when all the desired nodes are included in the area where you dragged the mouse
   - press the shift key and click on the nodes that are required to create the VPN.
4. Right click the mouse button while holding the shift key and select Start Tool -> Configuration -> Service Provisioning -> IP VPN Global Update.

The Select Customer and VPN dialog opens to let specify the customer and VPN to which you want to add the selected nodes.

The dialog contains a list of all the virtual routers (VRs) that you selected in the Network Viewer.



5 If you wish to use an existing customer, then select the customer name from the Customer Name drop down list. The list of VPNs for the selected customer appears in the VPN Name drop list.

If you wish to create a new customer, then select New Customer. The New Customer dialog opens. The VPN Name drop down list is empty.

In the New Customer dialog, complete the following tasks:

a. Enter a customer name in the Customer Name field.

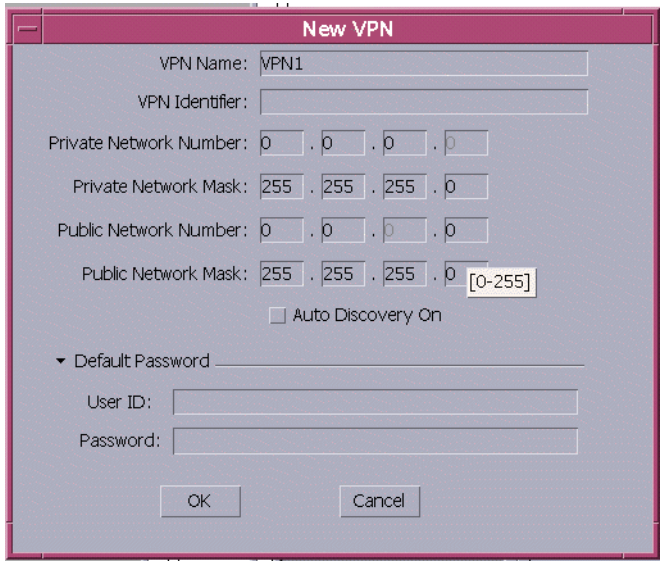
b. Enter a customer identifier in the Customer Identifier field.

c. Click OK.

the New Customer dialog closes. The name of the new customer is added to the customer list and is automatically selected.

6 If you wish to use an existing VPN, in the select customer and VPN dialog, select an existing VPN from the VPN Name drop down list.

If you wish to create a new VPN, in the select customer and VPN dialog, select the New VPN button. The New VPN dialog opens.



7 Enter a VPN name, identfier, User ID, and Password, and if desired, select Auto Discovery On.

8 Select OK to create the new VPN.

The dialog closes and the following occurs:

- the new VPN is added to the VPN Name drop down list and is selected

Note: If you selected an existing customer and VPN, and one of the nodes selected in the Network Viewer is already part of this VPN, that node is not added to the list since a switch can only have one virtual router per VPN.

9 In the Select Customer and VPN dialog, select OK.

- The IP VPN Global Update tool opens with the specified customer and VPN opened in the hierarchy tree
- A virtual router is created for every node that you selected in the Network Viewer

Starting the IP VPN global update tool (CLI)

You can access the IP VPN global update tool CLI from the Server Manager Administration tool.

1 Start the Server Manager Administration tool.

For the procedure to start the Server Manager Administration tool, see 241-6001-303 *Preside MDM Administrator Guide*.

2 Enter the appropriate IP VPN global update tool command from the command line.

Chapter 3
Installing the IP VPN global update tool

ATTENTION	If you have upgraded to Preside MDM Release 14.3, use the IP VPN Service Provisioning tool to configure RFC 2764 VPNs with auto-discovery enabled. See 241-6001-616 *Preside MDM IP VPN Service Configuration User Guide*. Further information can be found the the 14.3 Release Supplement.

For system requirements and installation instructions, see the following sections:

- "System requirements" (page 33)
- "Installing the IP VPN global update tool software" (page 34)
- "Updating the license" (page 34)

System requirements

The current supported platform of the IP VPN global update tool is SPARC Solaris.

The IP VPN global update tool requires the following software:

- Preside Multiservice Data Manager (MDM) software package. The IP VPN global update tool is part of the MDM package on the MDM CD-ROM.
- the following third-party software supplied by Nortel Networks on the MDM CD-ROM:
  - associated JRE patches for Solaris

- a valid license key

Installing the IP VPN global update tool software

For the IP VPN global update tool you need to install both Nortel Networks and third-party software from the Preside Multiservice Data Manager (MDM) CD-ROMs. Refer to the Release Supplement for the location of the required software.

Installing the IP VPN global update tool software involves the following installation procedures:

- "Installing and configuring MDM software" (page 34)
- "Updating the license" (page 34)

Installing and configuring MDM software

The IP VPN global update tool is part of the Preside Multiservice Data Manager (MDM) software package. When you load the Preside MDM software from CD-ROM with the InstallAnywhere program you When you load the Preside MDM software from CD-ROM with the InstallAnywhere program as described in 241-6001-100 *Preside MDM Installer Guide* you are instructed to:

- load the Solaris software patches for the Java Runtime Environment that is needed for the IP VPN global update tool
- load the Preside MDM software with the InstallAnywhere program. When you run the InstallAnywhere program to load the Preside MDM, the program automatically loads the software packages required for the. These packages are Preside MDM base and the Java Runtime Environment (JRE). You do not need to load any additional packages.

Updating the license

You need a license before you can run IP VPN global update for the first time. You only need to perform this procedure if the license you have for Preside MDM does not allow you to run IP VPN Global update.

Nortel Networks provides this information along with the Preside Multiservice Data Manager (MDM) software on the MDM CD-ROM. If you do not have this information, contact your Nortel Networks account representative.

To add the license key and customer identifier do the following:

1. Log in as root.
2. Using a UNIX editor open the following file for editing:

   `/etc/opt/Magellan/LIClicenses.cfg`
3. Add the license key to the file.
4. Check what you typed carefully.
5. Save the file and exit from it.
6. Open the following file for editing:

   `/etc/opt/Magellan/LICcustName.cfg`
7. Check what you typed carefully.
8. Save the file and exit from it.

Chapter 4
IP VPN global update tool GUI

For a description of the IP VPN global update tool graphical user interface (GUI), see the following sections:

- IP VPN global update tool main window
- IP VPN dialogs

IP VPN global update tool main window

The IP VPN GUI application consists of a main window from which you can initiate or perform provisioning tasks. The IP VPN global update GUI application lets you perform the following tasks:

- create a new customer
- remove a customer
- add a new VPN to a customer
- include VRs in the VPN
- add a VR to an existing VPN
- exclude a VR from an existing VPN
- apply IP CoS to a VPN

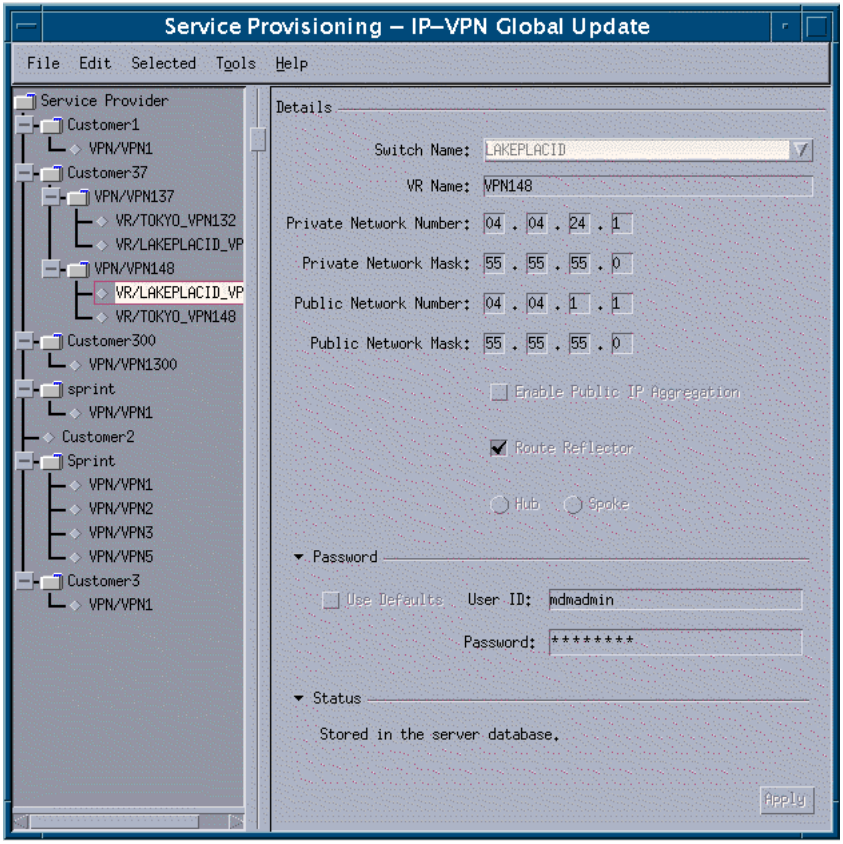
See also:

- “Options dialog” (page 56)
- “Confirm Provisioning Options dialog” (page 59)
- “Include VR dialog” (page 62)

- “CoS Policy Group dialog” (page 63)
- “Add New CoS Policy dialog” (page 66)
- “Modify CoS Policy dialog” (page 69)
- “New Flow Classification dialog” (page 71)
- “Modify Flow Classification dialog” (page 73)
- “Exclude VR dialog” (page 75)
- “Error and Message dialogs” (page 76)
- “Progress dialogs” (page 77)
- “Using the IP VPN global update tool GUI” (page 79)

For an illustration of the IP VPN global update tool main window, see the figure“IP VPN Global Update Tool main window with VR/ LAKEPLACID_VPN148 selected” (page 39).

Figure 2
IP VPN Global Update Tool main window with VR/LAKEPLACID_VPN148 selected



The IP VPN global update main window consists of the following elements:

- “Menu bar” (page 40)
- “Hierarchy tree panel” (page 43)
- “Details panel” (page 43)

Menu bar

The menu bar is located at the top of the IP VPN Global Update tool main window. It contains the following menu options:

- "File menu" (page 40)
- "Edit menu" (page 40)
- "Selected menu" (page 40)
- "Help menu" (page 43)

File menu

The File menu contains the following command:

- Exit
  Exit closes the IP VPN global update main window.

Edit menu

The Edit menu contains the following command:

- Options...
  Options... opens an Options dialog which displays a single provisioning tab where provisioning options may be edited. See "Options dialog" (page 56).

Selected menu

The commands that are available in the Selected menu vary with the item you select (service provider, customer, VPN, or VR) in the hierarchy tree. See the following sections:

- "Service provider selected menu" (page 41)
- "Customer selected menu" (page 41)
- "VPN selected menu" (page 41)
- "VR selected menu" (page 42)

Note: The Selected menu contains the same menu items as the pop-up menu that appears when you click the mouse menu button on an item in the hierarchy tree in the IP VPN global update main window.

Service provider selected menu

When you select service provider from the provisioning panel of the main window, the Selected menu contains the following command:

- Add new customer
  Add new customer adds a new customer to the service provider. The customer is created locally in the GUI tool. When you click Apply in the IP VPN global update main window, the customer is stored in the IP VPN server database.
- Help
  Help accesses the on-line documentation for the Service Provider Selected menu.

Customer selected menu

When you select a customer in the provisioning panel, the selected menu contains the following commands:

- Add new VPN
  Add new VPN adds a new VPN to the selected customer. The VPN is created locally in the GUI tool and is stored in the IP VPN server database when you click Apply in the main window.
- Remove
  Remove removes the selected customer from the IP VPN server database.

  Note: The Remove command is only available when the selected customer has no VPNs.

- Help
  Help accesses the on-line documentation for the Customer Selected menu.

VPN selected menu

When you select a VPN from the provisioning panel, the selected menu contains the following commands:

— Add new VRs
  Add new VRs opens the Include VR dialog. The Include VR dialog lets you add one or more new VRs to the selected VPN. See “Include VR dialog” (page 62).

— Remove
Remove removes the selected VPN from the IP VPN server database.

Note: This command is only available when the VPN that you have selected contains no VRs.

— Edit IP CoS...
Edit IP CoS opens the Edit Class of Service dialog. The Edit Class of Service dialog lets you create or modify the IP CoS for the selected VPN. See “CoS Policy Group dialog” (page 63).

— Help
Help accesses the on-line documentation for the VPN Selected menu.

VR selected menu

When you select a VR in the provisioning panel, the selected menu contains the following command:

- Remove
  Remove opens an Exclude VR dialog. The Exclude VR dialog lets you remove the selected VR from the containing VPN and from the IP VPN server database. See “Exclude VR dialog” (page 75).
- Help
  Helps accesses the on-line documentation for the VR Selected menu.

Tools menu

The Tools menu contains the following command:

- Nodal Provisioning
  Nodal Provisioning launches the Nodal Provisioning tool.

  Note: Once you launch the Nodal Provisioning tool, you can perform nodal provisioning tasks. However, before you can apply the service, you need to activate the provisioning changes in the nodal provisioning session and then close the Nodal Provisioning session. If you try to apply the service before you close the Nodal Provisioning tool, an error message appears saying that it can not start a provisioning session on the switch. The error message does not inform you that this error is generated because the Nodal Provisioning tool is holding the provisioning session.

Help menu

The Help menu contains the following commands:

- Help on Window
  Help on Window launches the online help information for the IP VPN Global Update tool main window.
- About IP-VPN Global Update
  About IP-VPN Global Update displays the GUI name and version information.

Hierarchy tree panel

The hierarchy tree panel is located on the left of the main window. When you start the IP VPN global update application, the hierarchy tree is populated with data retrieved from the IP VPN server database.

The hierarchy tree represents the containment hierarchy for IP VPN. The containment hierarchy consists of the service provider root and its service provider customers, customer VPNs and Virtual Routers (VR). You can expand or collapse items in the hierarchy tree that contain sub-items.

Details panel

The details panel, located to the right of the IP VPN global update main window, displays the provisioning data for the item that you select in the hierarchy tree. You can only select one item at a time from the hierarchy tree.

All the items in the hierarchy tree have a status which is displayed at the bottom of the details panel.

Note: No details are displayed on the Service Provider.

You can edit the information displayed in the details panel when the status displays the message that the item is “Not yet stored in the server database.” Items that have not yet been stored in the server database are items that are created through the GUI menu but have not yet been provisioned.

Once information is stored in the database, it cannot be modified.

Tooltips are available for each entry in the Details area. The tooltip text displays the valid values and ranges for each entry field. To access the tooltip, rest the mouse pointer over the entry field for two seconds.

An Apply command button is located the bottom right of the details panel. The Apply button is enabled when every required field in the details area contains a value.

For additional information see the following sections:

- “Customer details” (page 44)
- “VPN details” (page 46)
- “VR details” (page 51)

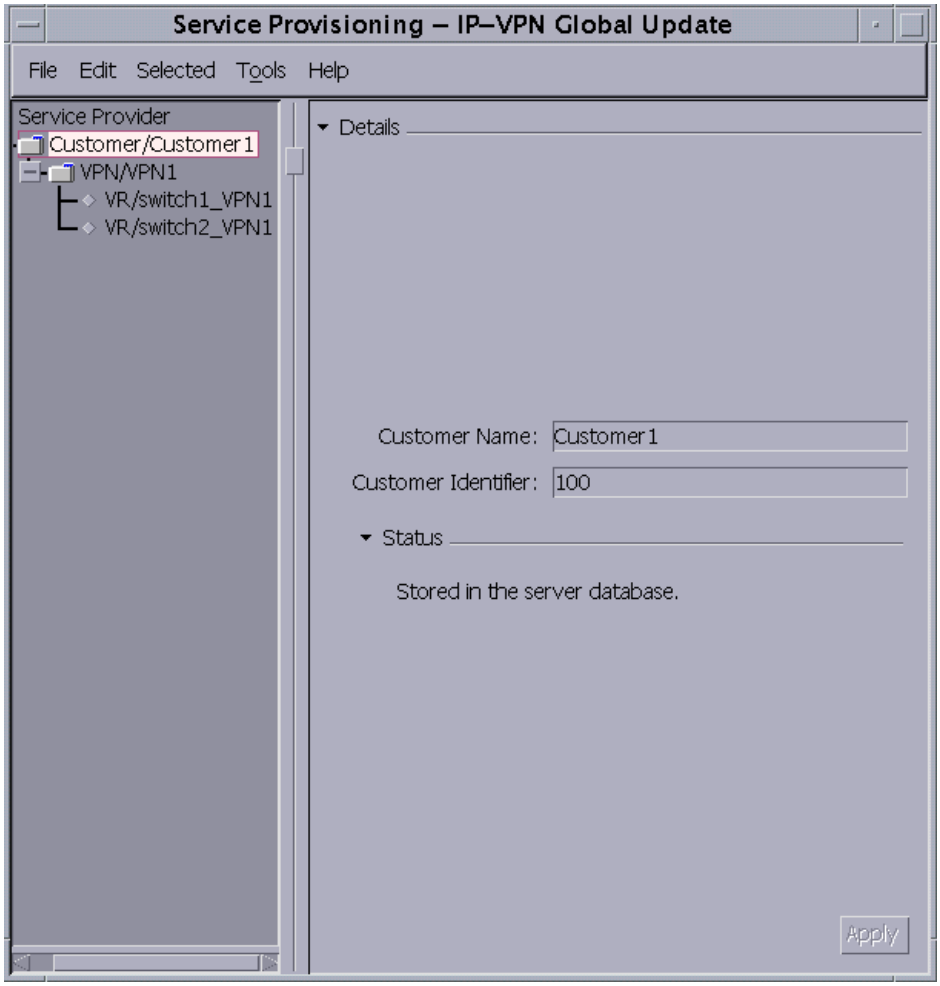
Customer details

The customer details panel lets you provision the customer that you have selected in the hierarchy tree in the IP VPN global update main window.When you select a customer in the hierarchy tree, the details panel displays the provisioning information on the selected customer.

The Apply command button in the customer details panel lets you initiates an action to store the customer in the IP VPN server database.

For an illustration of the details section, when a customer is selected, see the figure “Customer details area” (page 45)

Figure 3
Customer details area



For a summary of the customer properties, their defaults and their valid values, see the table “Customer details” (page 46).

Table 3
Customer details

Property	Description	Default value	Valid value or range
Name	The customer name	CustomerX, where X is an automatically incremented integer	A string containing a minimum of 1 ASCII character. Spaces are not allowed.
Identifier	The customer identifier	X, where X is an automatically incremented integer	An integer value in the range [0 - 8191]
Status	Indicates whether or not the customer has been stored in the server database	N/A	N/A

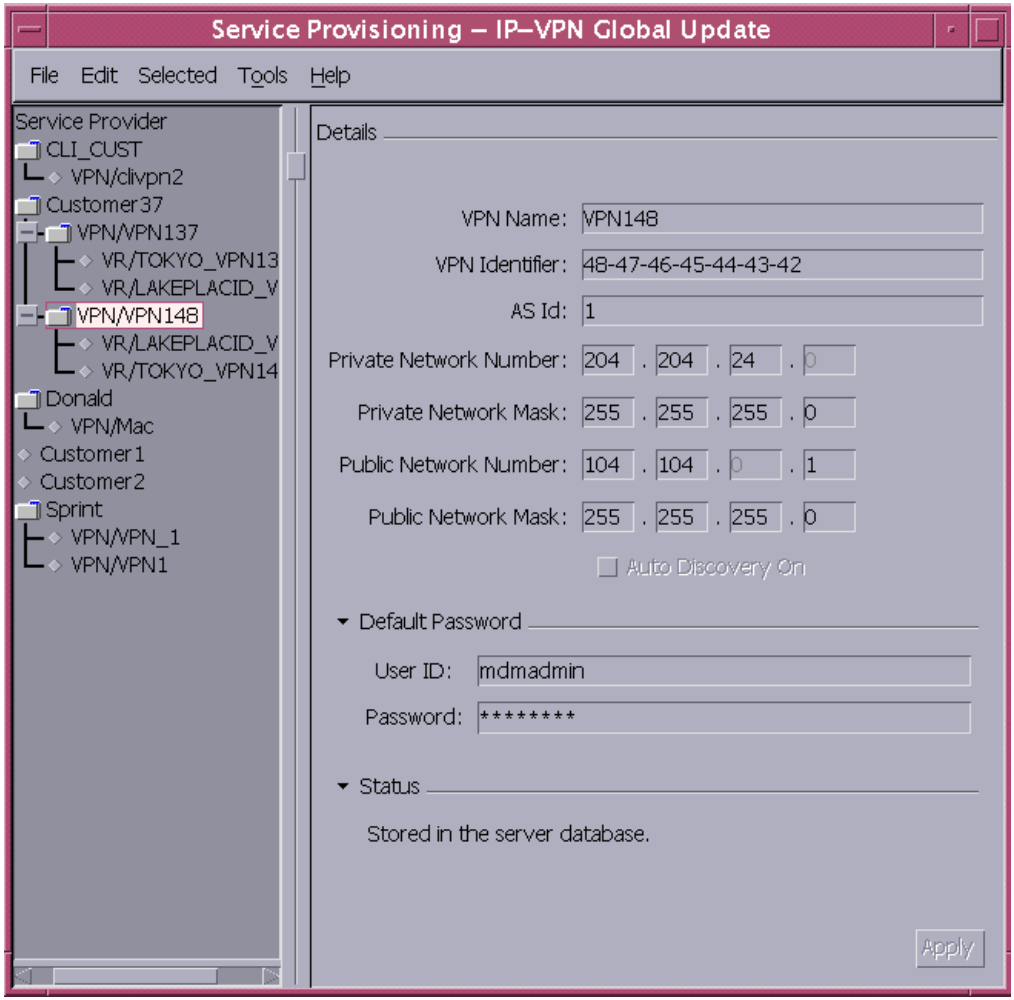
VPN details

The VPN details panel lets you provision the VPN that you have selected in the hierarchy tree in the IP VPN global update main window. When you select VPN in the hierarchy tree, the details area of the main window displays the provisioning information for the VPN.

The Apply command button in the VPN details panel initiates an action to store the VPN in the IP VPN server database.

For an illustration of the Details section, when a VPN is selected, see the figure“VPN details area” (page 47)

Figure 4
VPN details area



For a summary of the VPN properties and their valid values, see the table “VPN details” (page 48).

Table 4
VPN details

Property	Description	Default value	Valid value or range
Name	The VPN name	VPNX, where X is an automatically incremented integer	A string containing a minimum of 1 ASCII character. Spaces are not allowed.
Identifier	The VPN identifier	None	A dashed hex string consisting of 7 pairs of hex digits. The first 3 digits represent the 3-octet VPN authority Organizationally Unique Identifier and the following 4 digit pairs represent the 4 octet VPN index. Example: 11-12-13-14-15-16-17
AS Id	The Atonomous System identifier	1	[0...65535]
Auto Discovery On	The option to use the tool in Auto Discovery mode.	The check box is not selected	N/A
Private Network Number	A class C IP address that is used to form the class C part of the default private IP address for each VR included in the VPN. The last octet is incremented for each VR included in the VPN.	0.0.0.0	An IP address of the form [0-255].[0-255].[0-255].0

(Sheet 1 of 2)

Table 4 (continued)
VPN details

Property	Description	Default value	Valid value or range
Private Network Mask	A network mask that is used as the default network mask for the private IP address for each VR included in the VPN.	255.255.255.0	An IP address of the form [0-255].[0-255].[0-255].[0-255] representing a sequence of contiguous bits.
Public Network Number	An IP address that is used as the default public IP address for each VR included in the VPN	0.0.0.0	An IP address of the form [0-255].[0-255].[0-255].[0-255]
Public Network Mask	A network mask that is used as the default network mask for the public IP address for each VR included in the VPN	255.255.255.0	An IP address of the form [0-255].[0-255].[0-255].[0-255] representing a sequence of contiguous bits.
User ID	A default User identifier used to connect to the Passport device when provisioning the VPN	No default is supplied.	A string containing 1 to 8 ASCII characters
Password	A default password used to connect to the Passport device when provisioning the VPN	No default is supplied.	A string containing 5 to 8 ASCII characters
Status	Indicates whether or not the VPN has been stored in the server database.	N/A	N/A

(Sheet 2 of 2)

Auto Discovery

Selecting the Auto Discovery On check box in the VPN details panel provides the option to run the IP VPN Global Update tool in auto discovery mode. When auto discovery mode is selected, the Passport virtual routers (VRs) dynamically exchange the IP VPN topology information across VPN sites every time a customer VR is added or deleted.

All VRs in a VPN must be in either auto discovery mode or in static mode (not auto discovery mode).

> ***Note:*** Once you create a VPN in static mode, you cannot convert to auto discovery mode. When you add another VR to a VPN already in static mode, the Hub and Spoke radio button are disabled and the tool automatically creates the new VR in static mode. You need to recreate the IP VPN in auto discovery mode.

The VPN details provide default values for the VR details panel. There are two default addressing schemes:

- Private Network Number
- Public Network Number

AS Id

The AS Id field lets you specify a value for the atonomous system identifier (AS Id) of the VPN. All the VRs included in the same VPN have the same AS Id.

Private Network Number

For the Private Network Number, the VPN details panel requests a class C IP address. When you add a VR to the VPN, a class D IP address is provided as a default in the VR details panel for each VR. This class D address is generated by incrementing the last octet of the VPN's class C address by one for each VR added to the VPN. This simple strategy ensures that by default each VR in a VPN has a unique Private Network Number.

Public Network Number

For the Public Network Number, the VPN form requests an IP address with the third octet unspecified.

When you add VRs to the VPN, this IP address is supplied as the default Public Network Number value on the VR details panel. You must configure the Public Network Number for every VR on the same Passport node with the same class C Public Network Number. This permits class C address aggregation in the routing tables for the device and enables efficient use of the OSPF routing protocol across the backbone.

VR details

The VR details panel is used to provision the VR that you have selected in the hierarchy tree. The details area of the IP VPN Global Update Tool main window displays the provisioning data for the VR.

For a summary of the VR properties and their valid values, see the table "VR details" (page 54).

The VR details panel also contains the following items:

- a check box that lets you enable or disable public IP aggregation on switch
- a check box that let you specify that the VR is a route reflector in the VPN
- radio buttons that let you select whether the customer VR is a hub or spoke

If you select Enable Public IP Aggregation, you enable public IP aggregation on switch.

If you select the auto discovery mode, and also specify that the VR is a route reflector in the VPN, the Hub radio button is automatically selected, and is set to read-only mode.

If you do not specify that the VR is a route reflector, then you need to specify that the customer VR is either a hub or spoke. Based on the topology scenarios supported by the IP VPN Global Update tool, you have the following options:

- fully-meshed topology
  In a fully-meshed topology, all the customer VRs are hubs. The vpnPeering Topology attribute is set to hub on all the customer VRs

belonging to the VPN. Consequently, dynamic IBGP peers are set up to all other VPN sites. IP routes advertised by BGP instances of all VPN sites are known to all other VPN sites.

- star topology
  In a star topology, only one customer VR is specified as a hub and route reflector. All other customer VRs are spokes, and clients of the route reflector.
- star topology with two route reflectors
  In a star topology with two route reflectors, two customer VRs are specified as route reflectors and hubs. For each VR specified as a route reflector and hub, all the other VRs are its clients. The VRs not specified as route reflectors and hubs are spokes.

The Apply command button in the VR details panel opens a Confirm Provisioning Options dialog. For a description of the Confirm Provisioning dialog, see “Confirm Provisioning Options dialog” (page 59). The action to create and include the new VR in the VPN is only initiated when you click OK in the Confirm Provisioning Options dialog.

For an illustration of the VR details panel, see the figure “VR details panel” (page 53).

Figure 5
VR details panel

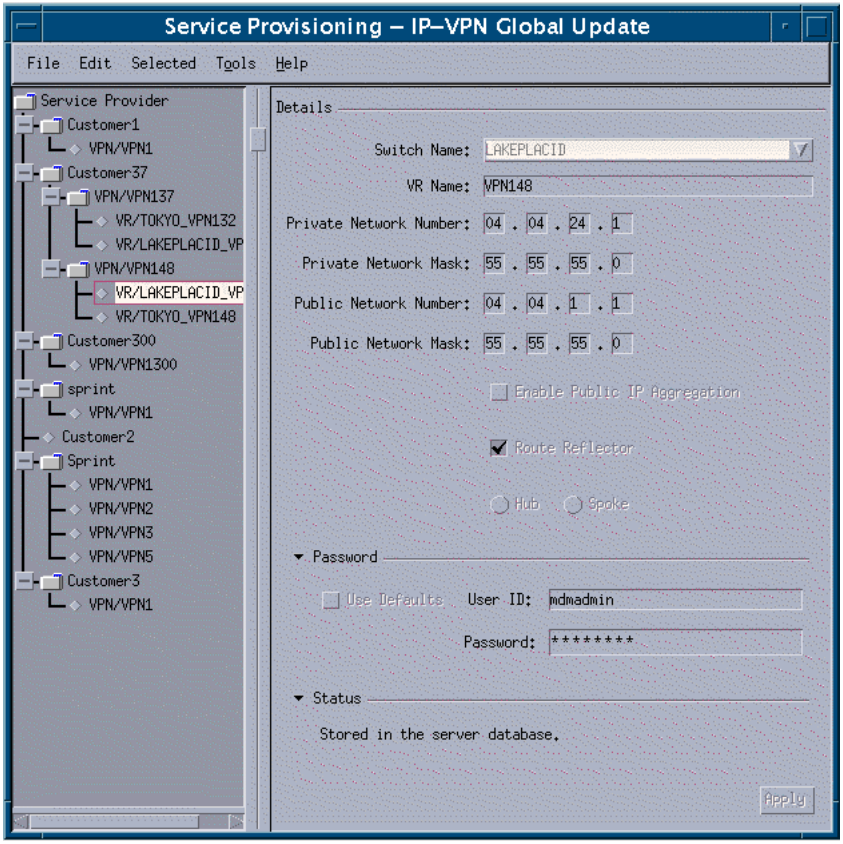


Table 5
VR details

Property	Description	Default value	Valid value or range
Switch Name	The name of the device on which the VR is provisioned	No default value.	The switch name must be present in the HGDS group.
Name	The VR name	The VPN to which the VR belongs is used as the default VR name.	A string containing 1 to 8 ASCII characters. Spaces are not allowed.
Private Network Number	The Private IP address for the VR.	The Private Network Number specified for the VPN with the last octet incremented with each VR included in the VPN.	An IP address of the form [0-255].[0-255].[0-255].[0-255]
Private Network Mask	A network mask of the private IP address for the VR.	The Private Network Mask specified for the VPN.	An IP address of the form [0-255].[0-255].[0-255].[0-255] representing a sequence of contiguous bits.
Public Network Number	An public IP address for the VR.	The Public Network Number specified for the VPN.	An IP address of the form [0-255].[0-255].[0-255].[0-255]
Public Network Mask	A network mask of the public IP address for the VR.	The Public Network Mask specified for the VPN.	An IP address of the form [0-255].[0-255].[0-255].[0-255] representing a sequence of contiguous bits.
Enable Public IP Aggregation	Indicates whether or not public IP aggregation on switch is enabled or disabled	No default value	Yes or No as indicated by the check box.

(Sheet 1 of 2)

Table 5 (continued)
VR details

Property	Description	Default value	Valid value or range
Route Reflector	Indicates whether or not the VR is a route reflector in the VPN.	No default value	Yes or No, as indicated by the check box.
Hub	Selects the customer VR as a hub in the VPN	Hub, when route reflector is selected	Yes or No, as indicated by the radio button.
Spoke	Selects the customer VR as a spoke in the VPN	No	Yes or No, as indicated by the radio button.
Password - Use Defaults	Indicates whether or not to use the default userid and password values supplied in the VPN.	By default, the “Use Defaults” option is selected.	The “Use Defaults” check box may be selected or unselected.
User ID	A User Identifier to connect to the Passport device when provisioning the VR.	No default is supplied.	A string containing 1 to 8 ASCII characters.
Password	A password used to connect to the Passport device when provisioning the VR.	No default is supplied	A string containing 5 to 8 ASCII characters.
Status	Indicates whether or not the VPN has been stored in the server database.	N/A	N/A

(Sheet 2 of 2)

IP VPN global update tool GUI dialogs

The IP VPN global update tool user interface generates the following dialogs:

- “Options dialog” (page 56)
- “Confirm Provisioning Options dialog” (page 59)
- “Include VR dialog” (page 62)

- “CoS Policy Group dialog” (page 63)
- “Add New CoS Policy dialog” (page 66)
- “Modify CoS Policy dialog” (page 69)
- “New Flow Classification dialog” (page 71)
- “Modify Flow Classification dialog” (page 73)
- “Exclude VR dialog” (page 75)
- “Error and Message dialogs” (page 76)
- “Progress dialogs” (page 77)

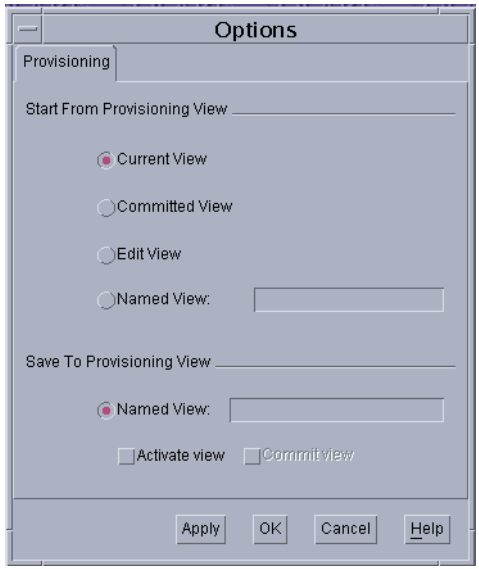
Options dialog

You access the Options editor dialog by clicking Options... in the Edit menu of the IP VPN global update tool main window. The Options dialog contains a single provisioning tab where provisioning options may be edited. The provisioning tab provides options for selecting a device view from which to start provisioning and a device view for saving provisioning data.

The Confirm Provisioning Options dialog contains similar options when an action resulting in on-switch provisioning is performed. The default values shown in the Confirm Provisioning Options dialog are those specified in t he provisioning tab of the Options dialog. See “Confirm Provisioning Options dialog” (page 59).

For an illustration of the Options dialog, see the figure “Options dialog” (page 57).

Figure 6
Options dialog



For a description of the parts of the Options dialog, see the following sections:

- “Start From Provisioning View” (page 57)
- “Save To Provisioning View” (page 58)
- “Command buttons” (page 58)

Start From Provisioning View

The Start From Provisioning View section provides the options for selecting a device view from which deferred to start provisioning. You can select from the following options by clicking the radio button:

- Current View
  Current View is the current configuration and operating parameters of the device.
- Committed View
  Committed View is the saved version of the current view that the devices uses when it resets or restarts.

- Edit View
  Edit View is the provisioning data which has been loaded into memory so that it can be modified.

- Named View
  Named View is a view stored in file with a user-specified filename. When you click Named View, the text box is activated so you can enter the file name of the view that you want to select. A valid file name is any ASCII string one to 31 characters long.

Save To Provisioning View

The Save To Provisioning View section lets you specify a file name for saving the provisioning data. When you click Named View you activate the text field. You must specify a file name in the text field. A valid file name is any ASCII string one to 31 characters long.

> ***Note:*** If you leave the Named View text field blank, the Apply and OK command buttons remain disabled.

The Save To Provisioning View area includes the following command buttons:

- Activate View
  Activate View activates the view that has been modified and saved during a provisioning session.

- Commit View
  Commit View commits the saved view. When you click the Activate view check box, the Commit view check box is activated so that you can commit the saved view.

Command buttons

The Options dialog has the following command buttons:

- Apply
  Apply applies the selected options.

- OK
  OK applies the selected options and closes the Options dialog.

- Cancel
  Cancel cancels the changes that you have made and closes the Options dialog.

- Help
  Help launches the online help information for the Options dialog.

Confirm Provisioning Options dialog

When you perform an action that results in on-switch provisioning, the Confirm Provisioning Options dialog opens to let you confirm or edit your provisioning options. The contents of the Confirm Provisioning Options dialog correspond to those found in the Options dialog. The default values shown in the Confirm Provisioning Options dialog are those that you selected in the Options dialog. See “Options dialog” (page 56).

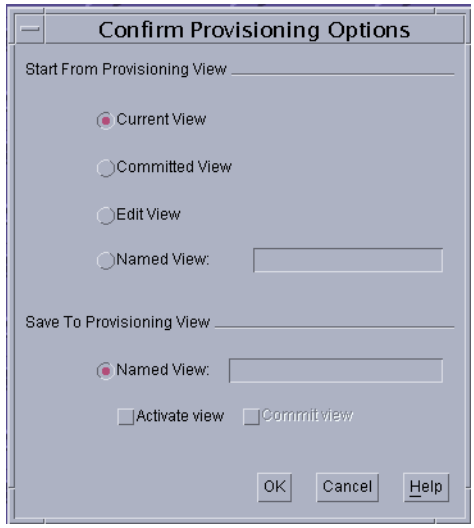
The Confirm Provisioning Options dialog opens when you perform the following actions:

- include a new VR in a VPN
- exclude a VR from a VPN
- apply IP CoS to a VPN

After performing an on-switch action, provisioning the device proceeds when you click OK in the Confirm Provisioning Options dialog.

For an illustration of the Confirm Provisioning Options dialog, see the figure “Confirm Provisioning Options dialog” (page 60).

Figure 7
Confirm Provisioning Options dialog



For a description of the parts of the Confirm Provisioning dialog, see the following sections:

- “Start From Provisioning View” (page 60)
- “Save To Provisioning View” (page 61)
- “Command buttons” (page 61)

Start From Provisioning View

The Start From Provisioning View section provides the options for selecting a device view from which to start provisioning. The default is the view that you selected in the Options dialog.

You can select from the following options by clicking the radio button:

- Current View
  Current View is the current configuration and operating parameters of the device.

- Committed View
  Committed View is the saved version of the current view that the devices uses when it resets or restarts.
- Edit View
  Edit View is the provisioned data currently being modified.
- Named View
  Named View is a view stored in file with a user-specified filename. When you click Named View, the text box is activated so you can enter the filename of the view that you want to select. A valid file name is any ASCII string that is one to 31 characters long.

Save To Provisioning View

The Save To Provisioning View section lets you specify a file name for saving the provisioning data. By default, the file name that you specified in the Options dialog appears in the Named View field.

The Save To Provisioning View area includes the following command buttons:

- Activate view
  Activate view activates the saved view.
- Commit view
  Commit view commits the saved view. When you click the Activate view check box, the Commit view check box is activated so that you can commit the saved view.

Command buttons

The Confirm Provisioning Options dialog has the following command buttons:

- OK
  OK causes the action which opened the Confirm Provisioning Options dialog to proceed by sending the appropriate requests to the IP VPN server. The server uses the specified provisioning options to begin provisioning the appropriate device or devices.
- Cancel
  Cancel cancels the operation which opened the Confirm Provisioning dialog.

- Help
  Help launches the online help information for the Confirm Provisioning Options dialog.

Include VR dialog

The Include VR dialog opens when you select a VPN in the hierarchy tree in the IP VPN global update main window and then select Add new VR from the VPN selected menu. The Include VR dialog lets you create and include a new VR in the VPN.

For an illustration of the Include VR dialog, see the figure “Include VR dialog” (page 62).

Figure 8
Include VR dialog

The Include VR dialog contains the following:

- “Create and Include New VRs text field” (page 62)
- “Command buttons” (page 62)

Create and Include New VRs text field

The Create and Include New VRs text field lets you specify the number of new VRs to create and include in the VPN. The default value is one.

Command buttons

The Include VR dialog has the following command buttons

- OK
  OK adds the number of VRs that you have specified in the text field to the VPN. Each VR is created locally in the GUI. To store the provisioning data in the IP VPN server database and to create the VRs you must click Apply in the IP VPN Global Update Tool window.

- Cancel
  Cancel cancels the Include VR operation.
- Help
  Help launches the online help for the Include VR dialog.

CoS Policy Group dialog

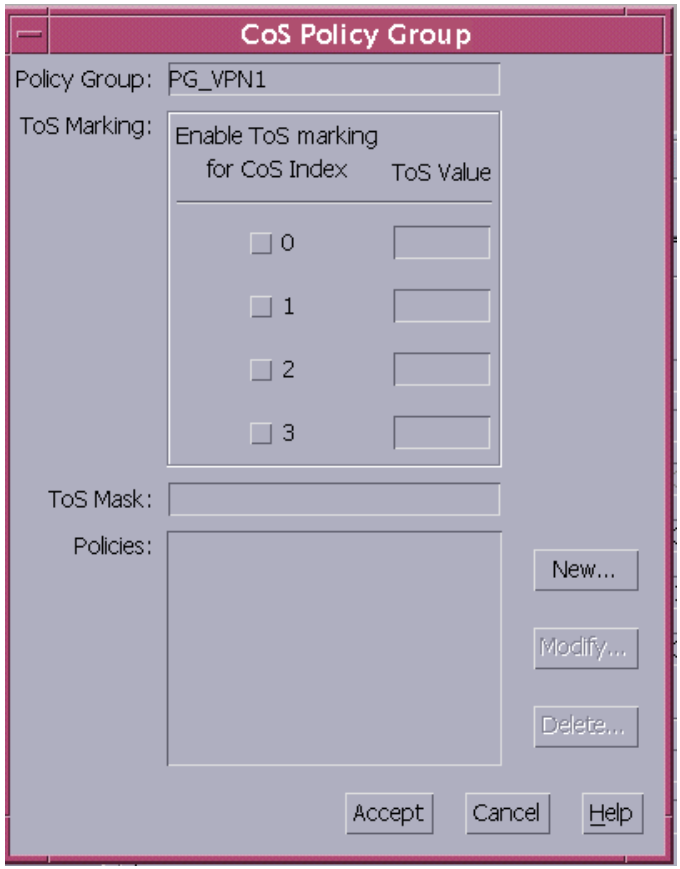
The CoS Policy Group dialog opens when you select Edit IP CoS... from the VPN Selected menu. You can provision the policy group, policies, and flow classifications that define the IP Class of Service for the VPN. A policy group contains zero or more policies and each policy contains zero or more flow classifications.

Provisioning IP CoS involves provisioning a single policy group for a VPN. This policy group applies across all VRs in that VPN. When a VR is added to a VPN with IP CoS already configured, the same policy group is applied to the new VR.

The IP CoS provisioning data is stored in the off-switch database on the IP VPN server. When the Edit Class of Service dialog is open for a VPN on which IP CoS has already been provisioned, the IP CoS data stored on the server is retrieved and displayed in the dialog. If the IP CoS data has not been previously provisioned, the dialog displays default values.

For an illustration of the CoS Policy Group dialog, see the figure “CoS Policy Group dialog” (page 64).

Figure 9
CoS Policy Group dialog



The CoS Policy Group dialog, has the following sections:

- “Policy Group field” (page 65)
- “Tos Marking panel” (page 65)
- “ToS Mask field” (page 65)
- “Policies list” (page 65)
- “Command buttons” (page 66)

Policy Group field

The Policy Group is the name of the policy group being provisioned. The default value is PG_<VPN name>. Valid values are a string containing one to 20 ASCII characters. Spaces are not allowed.

Tos Marking panel

The ToS Marking panel is used to provision ToS marking for the policy group. It has the following sections:

- Enable ToS marking for the CoS Index section provides check books that let you enable or disable the ToS marking for any of the CoS indices. By default, ToS marking is disabled for all CoS indices.
- ToS Value fields lets you specify a ToS value for each CoS index. Each ToS value is used with the ToS mask to determine the value of the ToS byte. The value fields can be blank or may contain a hexadecimal value from 00-FF. By default, the ToS value fields are blank.

ToS Mask field

The ToS Mask is the ToS bit mask that is used to determine the byte value. The Tos Mask field may be blank or contain any hexadecimal value from 00-FF.

Policies list

The Policies list contains a list of the policies that have been added to the policy group. By default, the Policies list is empty.

The contents of the list are modified using the following command buttons found to the right of the Policies list.

- New...
  New... opens an Add New CoS Policy dialog to add a new policy to the policy group. The new policy is added to the Policies list. See “Add New CoS Policy dialog” (page 66).
- Modify...
  Modify... opens a Modify CoS Policy dialog to edit the policy that is selected in the Policies list. The Modify... button is enabled only when a policy is selected from the list. See “Modify CoS Policy dialog” (page 69)

- Delete...
  Delete... removes the policy that is selected in the Policies list from the list.

Command buttons

The Edit Class of Service dialog has the follow command buttons:

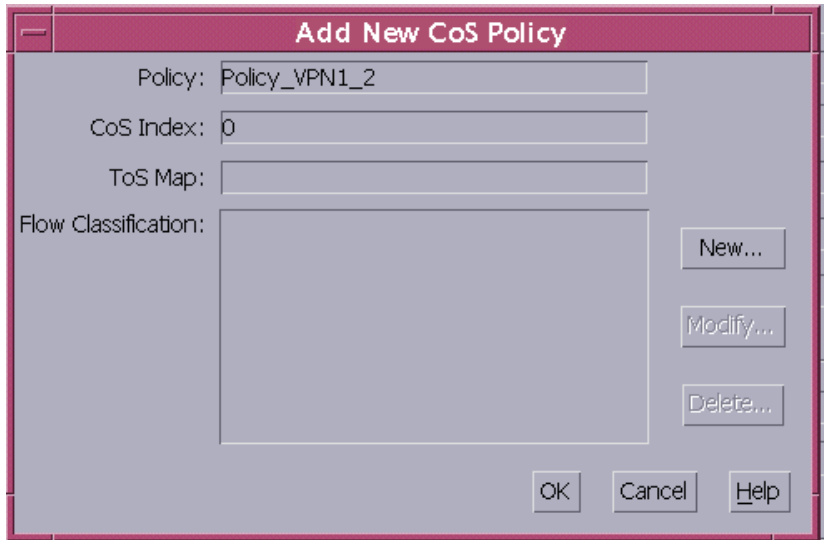
- Apply
  Apply opens a Confirm Provisioning Options dialog that lets you initiate the action to store the IP CoS provisioning data in the IP VPN Server database. The IP CoS is provisioned for any VRs contained in the VPN.
- Cancel
  Cancel erases the IP Cos provisioning data that you have entered and cancels the operation.
- Help
  Help launches the online help information for the CoS Policy Group dialog.

Add New CoS Policy dialog

The Add New CoS Policy dialog opens when you select New... in the Edit Class of Service dialog. The Add New CoS Policy dialog lets you provision a policy under a policy group.

For an illustration of the Add New CoS Policy dialog, see the figure “Add New CoS Policy dialog” (page 67).

Figure 10
Add New CoS Policy dialog



See the following for a description of the parts of the Add New CoS Policy dialog:

- “Policy field” (page 67)
- “CoS Index field” (page 67)
- “Tos Map field” (page 68)
- “Flow Classification list” (page 68)
- “Command buttons” (page 68)

Policy field

The Policy field specifies the name of the policy being provisioned. You can enter a string containing 1 to 20 ASCII characters. Spaces are not allowed. The default is Policy_<VPN name>_X, where X is incremented with the number of policies in the policy group.

CoS Index field

The CoS Index field identifies the class of service treatment a packet receives if this policy applies. Valid values is an integer in the range [0-3]. The default value is 0.

Tos Map field

The ToS Map field contains a list of ToS byte values used to map incoming packets under the same policy. Valid ToS values are a string of hexidecimals in the range [00-FF]. Each value must be separated by a space. By default, the ToS Map is empty.

Flow Classification list

The Flow Classification list contains a list of flow classifications that have been added to the policy. Command buttons to the right of the Flow Classification list let you modify the contents of the list:

- New...
  New... opens an Add Flow Classification dialog to add a new flow classification to the policy. When you add a new flow classification, it appears in the Flow Classification list.
- Modify...
  Modify... opens a Modify Flow Classification dialog to edit the flow classification that is selected in the Flow Classification list. The Modify... button is enabled when a flow classification is selected in the Flow Classification list.
- Delete...
  Delete... removes the flow classification that is selected in the Flow Classification list. The Delete button is only enabled when a flow classification is selected in the list.

Command buttons

The Add New CoS Policy dialog contains the following command buttons:

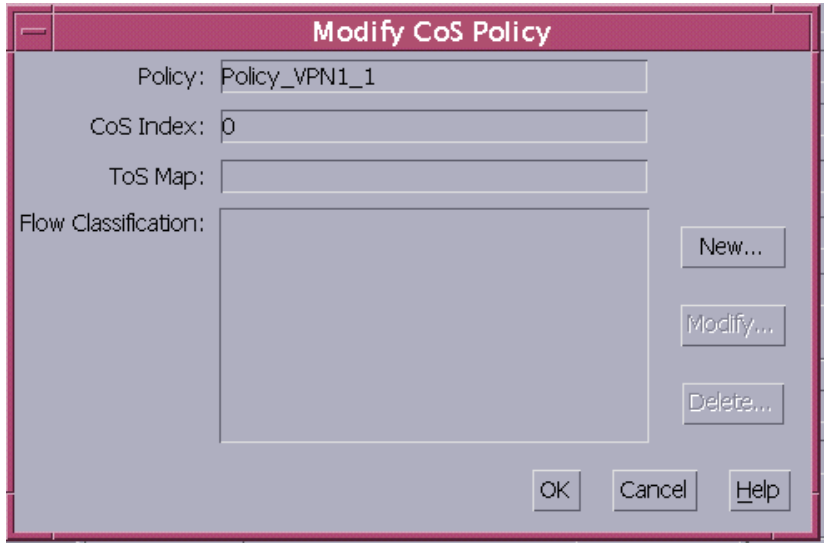
- OK
  OK adds the new Cos Policy to the policy group.
- Cancel
  Cancel cancels the operation.
- Help
  Help launches the online help information for the Add New CoS Policy dialog.

Modify CoS Policy dialog

The Modify CoS Policy dialog opens when you select a policy in the Edit Class of Service dialog and then select the Modify... command button. The Modify CoS Policy dialog lets you modify the provisioning data for the policy.

For an illustration of the Modify CoS Policy dialog, see the figure “Modify CoS Policy dialog” (page 69).

Figure 11
Modify CoS Policy dialog



See the following for a description of the parts of the Modify CoS Policy dialog:

- “Policy field” (page 70)
- “CoS Index field” (page 70)
- “Tos Map field” (page 70)
- “Flow Classification list” (page 70)
- “Command buttons” (page 71)

Policy field

The Policy field specifies the name of the policy being provisioned. You can enter a string containing 1 to 20 ASCII characters. Spaces are not allowed. The default is Policy_<VPN name>_X, where X is incremented with the number of policies in the policy group.

CoS Index field

The CoS Index field identifies the class of service treatment a packet receives if this policy applies. Valid values is an integer in the range [0-3]. The default value is zero.

Tos Map field

The ToS Map field contains a list of ToS byte values used to map incoming packets under the same policy. Valid ToS values are a string of hexidecimals in the range [00-FF]. Each value must be separated by a space. By default, the ToS Map is empty.

Flow Classification list

The Flow Classification list contains a list of flow classifications that have been added to the policy. Command buttons to the right of the Flow Classification list let you modify the contents of the list:

- New...
  New... opens an Add Flow Classification dialog to add a new flow classification to the policy. When you add a new flow classification, it appears in the Flow Classification list.
- Modify...
  Modify... opens a Modify Flow Classification dialog to edit the flow classification that is selected in the Flow Classification list. The Modify...button is enabled when a flow classification is selected in the Flow Classification list.
- Delete...
  Delete... removes the flow classification that is selected in the Flow Classification list. The Delete button is only enabled when a flow classification is selected in the list.

Command buttons

The Modify CoS Policy dialog contains the following command buttons:

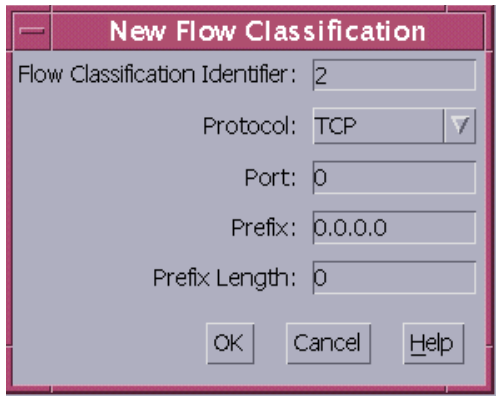
- OK
  OK updates the provisioning data for the policy that you selected in the Edit Class of Service dialog.
- Cancel
  Cancel cancels the operation.
- Help
  Help launches the online help information for the Modify CoS Policy dialog.

New Flow Classification dialog

The New Flow Classification dialog opens when you click New... in the Add New CoS Policy dialog or in the Modify CoS Policy dialog. The New Flow Classification dialog lets you provision a flow classification for a policy.

For an illustration of the New Flow Classification dialog, see the figure "New Flow Classification dialog" (page 71).

Figure 12
New Flow Classification dialog



For the parts of the New Flow Classification, see the following sections:

- "Flow Classification Identifier field" (page 72)
- "Protocol field" (page 72)

- "Port field" (page 72)
- "Prefix field" (page 72)
- "Prefix length field" (page 72)
- "Command buttons" (page 72)

Flow Classification Identifier field

The Flow Classification Identifier field lets you enter a flow classification identification. It is an integer in the range [0-1023]. By default it is an integer that is incremented with the number of flow classifications in the policy group.

Protocol field

The protocol field lets you specify the layer 4 protocol used to distinguish incoming packets under the same policy. You can select from a drop-down list containing the following protocols; TCP, UDP or ICMP. The default is TCP.

Port field

The port field lets you specify the single layer 4 port number used to distinguish incoming packets under the same policy. The valid range is an integer in the range [0-65535]. The default value is 0.

Prefix field

Prefix is an IP address used to match incoming packets under the same policy. An IP address is of the form [0-255].[0-255].[0-255].[0-255]. 0.0.0.0 is the default.

Prefix length field

Prefix length is the number of most significant bits in the Prefix that are used to match the IP address of an incoming packet. Valid values are integers in the range [0-32]. The default value is 0.

Command buttons

The dialog has the following command buttons:

- OK
  OK adds the flow classification to the policy group.
- Cancel
  Cancel cancels the add a new flow classification operation.

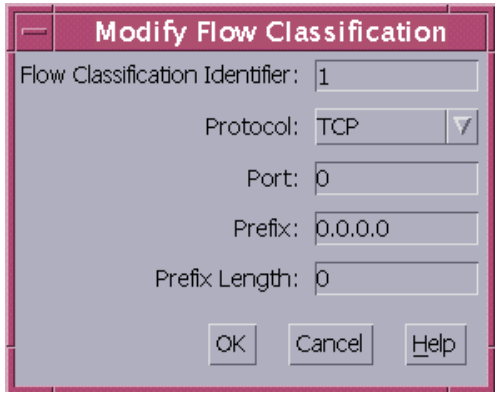
- Help
  Help launches the online help information for the New Flow Classification dialog.

Modify Flow Classification dialog

The Modify Flow Classification dialog opens when you select Modify... in the Add New CoS Policy dialog or in the Modify CoS Policy dialog. You can modify the flow classification for a policy using the Modify Flow Classification dialog.

For an illustration of the modify flow classification dialog, see “Modify Flow Classification dialog” (page 73).

Figure 13
Modify Flow Classification dialog



The Modify Flow Classification dialog contains the same fields as the Add Flow Classification. See the following sections:

- “Flow Classification identifier field” (page 74)
- “Protocol field” (page 74)
- “Port field” (page 74)
- “Prefix field” (page 74)
- “Prefix length field” (page 74)
- “Command buttons” (page 74)

Flow Classification identifier field

The Flow Classification Identifier field lets you enter a flow classification identification. It is an integer in the range [0-1023]. By default it is an integer that is incremented with the number of flow classifications in the policy group.

Protocol field

The Protocol field lets you specify the layer 4 protocol used to distinguish incoming packets under the same policy. You can select from a drop-down list containing the following protocols; TCP, UDP or ICMP. The default is TCP.

Port field

The port field lets you specify the single layer 4 port number used to distinguish incoming packets under the same policy. The valid range is an integer in the range [0-65535]. The default value is 0.

Prefix field

Prefix is an IP address used to match incoming packets under the same policy. An IP address is of the form [0-255].[0-255].[0-255].[0-255]. 0.0.0.0 is the default.

Prefix length field

Prefix length is the number of most significant bits in the Prefix that are used to match the IP address of an incoming packet. Valid values are integers in the range [0-32]. The default value is 0.

Command buttons

The dialog has the following command buttons:

- OK
  OK updates the provisioning data for the flow classification that was selected in the Add New CoS Policy dialog.
- Cancel
  Cancel cancels the modify flow classification operation.
- Help
  Help launches the online help for the Modify Flow Classification dialog.

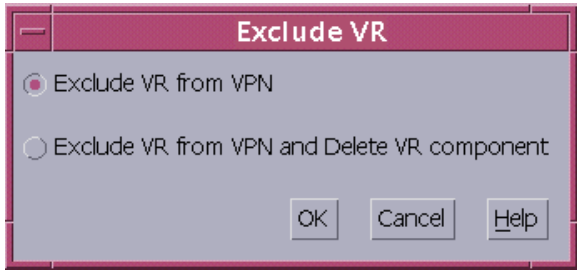
Exclude VR dialog

The Exclude VR dialog opens when you select a VR in the IP VPN Global Update Tool window and then select Remove from the VR selected menu. The Exclude VR dialog lets you remove a VR from the VPN.

> ***Note:*** You can only access the VRs that were added to a VPN by using the IP VPN global update tool.

For an illustration of the Exclude VR dialog, see the figure "Exclude VR dialog" (page 75).

Figure 14
Exclude VR dialog



The Exclude VR dialog contains the following options:

- Exclude VR from VPN
  The Exclude VR from VPN radio button excludes the VR from the VPN that contains it. The VR component is not deleted but it is no longer part of any VPN.
- Exclude VR from VPN and Delete VR component
  The Exclude VR from VPN and Delete VR component radio button excludes the VR from the VPN that contains it and deletes the VR component from the device on which it has been provisioned.

The Exclude VR dialog contains the following command buttons:

- OK
  OK opens the Confirm Provisioning Options dialog. See “Confirm Provisioning Options dialog” (page 59). The exclude VR operation proceeds when you click OK in the Confirm Provisioning Options dialog.
- Cancel
  Cancel cancels the exclude VR operation.
- Help
  Help launches the online help information for the Exclude VR dialog.

Error and Message dialogs

Information and errors are displayed in message dialogs. Message dialogs contain an OK button. When you select the OK button, the message dialog closes.

An error message dialog opens in the following situations:

- IP VPN server is not running while the tool is connecting. The Message dialog opens with the message “Shutting down...Unable to connect to the server... IP VPN Server not responding.
- IP VPN server shuts down while the tool is connected. The dialog opens with the message “The connection to the IP VPN Server has been lost. Shutting down...”.
- Failure to obtain a list of devices from HGDS. The message dialog opens with the message “Unable to retrieve the device names. Reason...”. The reason is that reported by the server.
- Invalid data has been entered in any entry field and an attempt is made to apply the provisioning data. A message dialog opens indicating which field is invalid and what the valid values are.
- Failure of any provisioning operation on the device, including check prov failures. The device error text is reported verbatim in a message dialog

See the figure “Example of a message dialog” (page 77) for an illustration of the message dialog that opens when you cannot connect to the server.

Figure 15
Example of a message dialog

Log files

A log file may be specified in the IP_VPN_Client.txt configuration file using the following syntax:

```
log_file=<filename>
```

where:

`<filename>` is the fully specified path and filename for the log file. The path to the filename must exist for logging to be recorded in the file. The following items are recorded in the log file:

- state information, including information about the state of the connection to the IP VPN server
- records of any configuration operations initiated by the user
- text that is displayed in any error message dialogs

Progress dialogs

A progress dialog opens when the IP VPN global update tool communicates with the IP VPN server. The dialog indicates what action is being performed and its progress. When the action is complete, the progress dialog closes.

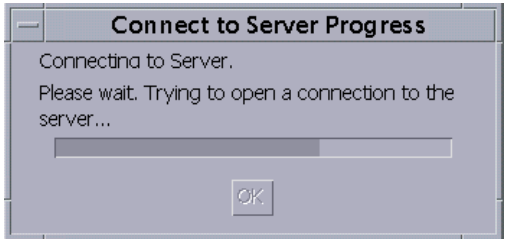
Progress dialogs open in the following situations:

- IP VPN global update GUI start-up while the GUI connects to the server and retrieves data stored in the server database
- applying or removing a customer
- applying or removing a VPN

- applying or excluding a VR
- applying IP CoS

See the figure “Example of a progress dialog” (page 78) for an example of the progress dialog that opens when you connect to the server.

Figure 16
Example of a progress dialog



Chapter 5
Using the IP VPN global update tool GUI

ATTENTION	If you have upgraded to Preside MDM Release 14.3, use the IP VPN Service Provisioning tool to configure RFC 2764 VPNs with auto-discovery enabled. See 241-6001-616 *Preside MDM IP VPN Service Configuration User Guide*. Further information can be found the the 14.3 Release Supplement.

For the procedures to use the IP VPN global update tool GUI, see the following sections:

- "Selecting a device view for provisioning, and saving provisioning data" (page 79)
- "Service provider selected menu procedures" (page 80)
- "Customer selected menu procedures" (page 81)
- "VPN selected menu procedures" (page 83)
- "VR selected menu procedures" (page 90)
- "Creating a new customer VPN" (page 91)

Selecting a device view for provisioning, and saving provisioning data

The Options dialog provides options to select a device view from which to start provisioning, and to specify the file name to save the provisioning data. You can specify or change the provisioning options at any time during your provisioning session.

Note: For any action that results in on-switch provisioning, the Confirm Provisioning Options dialog opens before provisioning proceeds. If you have already specified the provisioning options, the default values displayed in the Confirm Provisioning Options dialog correspond to the values that you specified in the Options dialog. The Confirm Provisioning Options dialog lets you confirm or edit your selections.

1. In the IP VPN global update main window, select Edit.
2. From the Edit menu, select Options...

   The Options dialog opens. See “Options dialog” (page 56) for a description of the dialog.
3. In the Start From Provisioning View area, select a device view from which to start provisioning. You have see “Start From Provisioning View” (page 60).
4. To save the provisioning data to a file, in the Save To Provisioning View area click Named View and enter the appropriate provisioning data file information in the Named View field. See “Save To Provisioning View” (page 61).
5. To activate the modified view, click Activate view.

   The Commit view is enabled.
6. To commit the view, click Commit view.
7. To apply the selected options, click Apply.

   To apply the selected options and close the Options dialog, click OK.

   To cancel the selections and close the Options dialog, click Cancel.

Service provider selected menu procedures

From the service provider selected menu, you can add a new customer to the service provider. See “Adding a new customer” (page 80).

Adding a new customer

1. Launch the IP VPN global update tool.

   The tool opens with all customer and associated VPN data loaded in the hierarchy.
2. In the hierarchy tree, click the mouse menu button on Service Provider.
3. From the pop-up menu, select Add new customer.

The new customer appears at the bottom of the hierarchy with the name Customer/CUSTOMER<n>.

4 In the hierarchy, select the newly created customer.

The Details panel is populated with the default information for the customer.

5 In the Details panel, complete the following:

a. In the Customer Name field, enter a valid customer name.

b. In the Customer Identifier field, enter a valid customer identifier.

See “Customer details” (page 46) for information on valid values and ranges.

The Apply button is enabled when all fields are filled in.

Note: You can obtain tooltip information on the fields by placing the mouse pointer over the field.

6 Click Apply to add the customer to the server database.

If the data that you have entered is valid, a create customer progress dialog opens showing the progress of the Add new customer command. Click OK. If the operation succeeds, the Apply button is disabled and the Customer status section of the Details panel indicates that the details are “stored in the server database”. The hierarchy tree is updated to contain the new customer.

If any of the data entered in the Details panel are invalid, an error dialog opens indicating which field is invalid and why. Return to step 5 to enter valid data.

Customer selected menu procedures

From the customer selected menu, you can perform the following customer-related procedures:

- “Removing a customer” (page 81)
- “Adding a new VPN to a customer” (page 82)

Removing a customer

You can remove a customer from the service provider.

Note: The Remove command is only available when the selected customer has no VPNs.

1. In the IP VPN global update tool main window, expand the hierarchy to display the customer that you want to remove.
2. Click the mouse menu button on the Customer that you want to remove from the hierarchy.
3. From the pop-up menu, select Remove.

   A Delete Customer Progress dialog appears telling you that the customer is being deleted.
4. Click OK.

   The customer is removed from under Service Provider in the hierarchy tree.

Adding a new VPN to a customer

You can add a new VPN to a customer.

1. In the IP VPN Global Update Tool main window, expand the hierarchy to display the customer to which you want to add a VPN.
2. Click the mouse menu button on the customer to which you want to add a VPN.
3. From the pop-up menu, select Add new VPN.

   A new VPN appears under the selected customer.
4. In the hierarchy, select the VPN that you have created.

   The Details panel displays the default information for the VPN.
5. Edit the VPN Name and VPN Identifier fields in the VPN Details panel if required.

   The VPN identifier is a hex string consisting of 7 pairs of hex digits. The first three digits represent the 3-octet VPN authority Organizationally Unique Identifier and the following four digit pairs represent the 4-octet VPN index.

   Note: You can access tooltips on the valid values and ranges by placing your mouse pointer over a field.
6. To use the tool in auto discovery mode, select the Auto Discovery On check box.
7. Edit the remaining fields in the VPN Details panel, if required.

   See “VPN details” (page 48) for a description of the fields and the valid values and ranges.

Data common to all VRs in the VPN can be configured here, and this data is used to provide defaults in the VR details panel for VRs that may later be included in the VPN. As a default value, the last octet of the private network number is incremented for each VR that is included in the network. The private network mask, public network number, and public network mask values are used unchanged as default values for VRs that are included in the VPN. The default userid and password values can also be applied to VRs included in this VPN.

The Apply button is enabled when all the fields are filled in. See “VPN details” (page 48) for a description of the fields and the valid values and ranges.

8 Click Apply to add the VPN information to the server database.

One of the following occurs:

- If all of the data entered in the Details fields is valid, a progress dialog opens showing the progress of the Add new VPN command. When the operation is successfully completed, Apply is disabled and the Status changes to “Stored in the server database”. The customer in the hierarchy tree is updated with the VPN.
- If the data entered in any of the fields is invalid, a message dialog appears indicating which field is invalid and why. Correct the invalid data and click Apply.
- If an error occurs while the operation is in progress, a message dialog opens indicating the error, and the Add new VPN operation ends.

VPN selected menu procedures

From the VPN Selected menu, you can perform the following procedures:

- “Adding a VR to a VPN” (page 83)
- “Removing a VPN” (page 85)
- “Applying IP CoS to a VPN” (page 86)

Adding a VR to a VPN

You can add VRs to a VPN. This procedure describes adding VRs to an existing VPN. See “Creating a new customer VPN” (page 91) for the procedure to include VRs in a new VPN.

1 In the IP VPN global update tool window, expand the hierarchy to display the VPN to which the new VR is to be added.

2 Click the mouse menu button on the VPN to which you want to add a VR.

3 From the pop-up menu, select Add new VRs.

The Include VR dialog opens.

4 In the Create and Include New VRs text field, enter the number of VRs that you want to include in the VPN.

5 Click OK.

The VRs are added to the selected VPN.

6 From the hierarchy tree, select the first of the newly added VRs

The default information on the VR appears in the fields in the Details panel.

7 Edit the default information contained in the fields (Switch Name, VR Name, Private Network Number, Private Network Mask, Public Network Number, Public Network Mask, Enable Public IP Aggregation, and Route Reflector), if required, and enter a valid User ID and Password. See “VR details” (page 54) for a description of the fields and their valid values and ranges.

Note 1: The “Switch Name” combo box contains a drop down list of all possible device names.

Note 2: You can access tooltips that provide valid values and ranges for the field by placing your mouse pointer over the field.

8 If the VPN containing the VR being added has Auto Discovery set, proceed to step 9.

If the VPN containing the VR being added does not have Auto Discovery set, proceed to step 10.

9 Complete one of the following steps:

- select Route Reflector. If you select Route Reflector, the hub radio button is automatically selected and set to read-only mode.
- do not select Route Reflector. If you do not select Route Reflector then you must select either hub or spoke.

The Apply button is enabled when you have filled in all the fields.

10 Click Apply to add the VPN to the server database.

If any of the data entered in the details panel is invalid, a message dialog opens indicating which field is invalid and why. Correct the invalid data and Click Apply again.

If all of the data is valid, a Confirm Provisioning Options dialog opens. See “Confirm Provisioning Options dialog” (page 59).

11 To select a device view from which to start provisioning, in the Start From Provisioning View area, select a device view.

12 To specify a file name to save the provisioning view, in the Save To Provisioning View area, click the Named View radio button and enter a name in the text field.

13 To activate the saved view, click Activate view.

Commit view is activated.

14 To commit the view, click Commit view.

15 Click OK.

A progress dialog appears showing the progress of the create and include VR command.

If the operation is successful, the Apply button is disabled and the status message in the details panel changes to “Stored in the server database”.

If an error occurs while the operation is in progress, a message dialog opens that indicates the error. The operation stops and the tool disconnects for any devices that it is connected to.

16 Repeat steps 6 to 14 for each VR that you added to the VPN.

Note: When you display the data input fields for the next VR that you create, the Private Network Number is automatically incremented.

Removing a VPN

You can remove a VPN from a customer.

Note: The Remove command is enabled only if the VPN does not contain VRs.

1 In the IP VPN global update tool main window, expand the hierarchy to display the VPN that you want to remove.

2 Click the mouse menu button on the VPN that you want to remove and select Remove.

A Delete VPN Progress window appears.

The VPN is no longer listed under the customer.

Applying IP CoS to a VPN

You can provision the policy group, policies and flow classifications that define the IP CoS for the VPN. See the following for the procedures to apply IP CoS to the VPN or to change the IP CoS configured for the VPN:

- "Opening the Edit Class of Service dialog" (page 86).
- "Provisioning the CoS policy group" (page 86).
- Adding modifying, or deleting policies.
  - To add a policy, see "Adding a policy" (page 87)
  - To modify an existing policy in the policy group, see "Modifying a policy" (page 87)
  - To delete a policy from a policy group, see "Deleting a policy" (page 88).
- Adding, modifying, or deleting flow classifications in a policy
  - to add a flow classification, see "Adding a flow classification" (page 88)
  - to modify a flow classification, see "Modifying a flow classification" (page 89)
  - to delete a flow classification, see "Deleting a flow classification" (page 89).
- Applying the provisioning changes. See "Applying IP CoS provisioning changes" (page 90).

Opening the Edit Class of Service dialog

1. In the IP VPN global update tool main window, expand the hierarchy to display the VPN to which you want to apply the IP CoS.
2. Click the mouse menu button on the VPN.
3. From the pop-up menu, select Edit IP CoS...

   The Edit Class of Service dialog opens. See "CoS Policy Group dialog" (page 63).

Provisioning the CoS policy group

1. In the Edit Class of Service dialog fields, as required, enter a Policy Group name, set each CoS Index check box, provide a ToS Marking value and enter a ToS Mask.

2 Proceed to one of the following procedures:

To apply the changes, see “Applying IP CoS provisioning changes” (page 90)

To add a policy to the policy group, see “Adding a policy” (page 87).

To modify a policy in the policy group, see “Modifying a policy” (page 87).

To delete a policy from the policy group, see “Deleting a policy” (page 88).

Adding a policy

You can add a new policy to the policy group

1 In the Edit Class of Service dialog, click New...

The Add New CoS Policy dialog opens. See “Add New CoS Policy dialog” (page 66).

2 Edit the Policy, CoS Index, and ToS Map fields, as required.

3 Proceed to one of the following procedures.

Click OK and proceed to “Applying IP CoS provisioning changes” (page 90) to apply the changes.

Note: If any of the data entered in the fields is invalid, a message dialog opens indicating which field is invalid and why. Correct the data and click OK again.

To add a flow classification, see “Adding a flow classification” (page 88).

To modify a flow classification, see “Modifying a flow classification” (page 89).

To delete a flow classification, see “Deleting a flow classification” (page 89).

Modifying a policy

You can edit a policy in the policy group from the Edit Class of Service dialog.

1 From the Policies list in the Edit Class of Service dialog, select the policy that you want to modify

2 Click Modify...

The Modify CoS Policy dialog opens. See “Modify CoS Policy dialog” (page 69).

3 Edit the Policy, CoS Index, and ToS Map fields, as required.

4 Proceed to one of the following procedures:

Click OK to close the Modify CoS Policy dialog and proceed to "Applying IP CoS provisioning changes" (page 90).

Note: If any of the data entered in the fields is invalid, a message dialog opens indicating which field is invalid and why. Correct the data and click OK again.

To add a flow classification to the policy, see "Adding a flow classification" (page 88).

To modify a flow classification, see "Modifying a flow classification" (page 89).

To delete a flow classification, see "Deleting a flow classification" (page 89).

Deleting a policy

You can delete a policy from a policy group from the Edit Class of Service dialog.

1 In the Policies list in the Edit Class of Service dialog, select the policy that you want to remove.

2 Click Delete...

The policy is removed from the Policies list.

3 To apply the changes see "Applying IP CoS provisioning changes" (page 90).

Adding a flow classification

You can add a flow classification to the policy from the Add New CoS Policy and the Modify CoS Policy dialogs.

1 In the Add New CoS Policy or Modify CoS Policy dialog, click New...

An Add Flow Classification dialog opens.

2 Enter values in the Flow Classification Identifier, Port, Prefix and Prefix Length fields, and select a Protocol from the drop down list.

3 Click OK to close the Add Flow Classification dialog.

Note: If any of the data entered in the fields is invalid, a message dialog opens indicating which field is invalid and why. Correct the data and click OK again.

4 Click OK to close the Add New CoS Policy dialog.

The Edit Class of Service dialog remains open.

5 Proceed to “Applying IP CoS provisioning changes” (page 90).

Modifying a flow classification

You can modify an existing flow classification in a policy by launching the Modify Flow Classification dialog from the Add New CoS Policy or Modify CoS Policy dialogs.

1 From the Flow Classification list in the Add New CoS Policy or Modify CoS Policy dialog, select the flow classification that you want to modify.

2 Select Modify...

A Modify Flow Classification dialog opens.

3 Edit the Flow Classification Identifier, Port, Prefix, and Prefix Length fields and select a Protocol from the drop-down list.

4 Click OK to close the Modify Flow Classification dialog.

Note: If any of the data entered in the fields is invalid, a message dialog opens indicating which field is invalid and why. Correct the data and click OK again.

5 Click Ok to Close the Add New CoS Policy or Modify CoS Policy dialog.

The Edit Class of Service dialog remains open.

6 Proceed to “Applying IP CoS provisioning changes” (page 90).

Deleting a flow classification

You can delete an existing flow classification from a policy.

1 From the Flow Classification list in the Add New CoS Policy or Modify CoS Policy dialog, select the flow classification that you want to delete.

2 Select Delete...

The selected flow classification is removed from the Flow Classification list.

3 Click OK to close the Add New CoS Policy or Modify CoS Policy dialog.

The Edit Class of Service dialog remains open.

4 Click Apply.

An Edit Policy Group progress dialog opens.

5 Click OK.

Applying IP CoS provisioning changes

1 In the Edit Class of Service dialog, click Apply.

The Confirm Provisioning dialog opens.

Note: New VRs subsequently added to the VPN will have this policy group applied to them.

Note: The Confirm Provisioning dialog does not open when there are no VRs in the VPN.

If any of the data entered in the details panel is invalid, a message dialog opens indicating which fields are invalid. Correct any invalid data and click Apply again.

2 In the Confirm Provisioning dialog, select the provisioning views that you would like to start from and save to, the select the Activate view and Commit view as desired.

3 Click OK.

A progress dialog opens showing the progress of the Apply CoS command.

Note: If an error occurs while the operation is in progress, a message dialog opens that indicates the error. The operation stops and the tool disconnects from any devices to which it is connected.

VR selected menu procedures

From the VR selected menu, you can exclude a VR from a VPN and delete the VR component.

Excluding or deleting a VR from an existing VPN

1 In the IP VPN global update tool main window, expand the hierarchy to display the VR you wish to remove.

2 Click the mouse menu button on the VR that you want to remove.

3 From the pop-up menu, select Remove.

The Exclude VR dialog opens.

4 To exclude the VR from VPN, select Exclude VR from VPN and click OK. The VR component is not deleted from the device.

To remove the VR from VPN and delete the VR component from the device on which it has been provisioned, select Exclude VR from VPN and Delete VR component and click OK.

5 A Confirm Provisioning Options dialog opens.

6 Confirm or edit the Save From Provisioning View options and Save to Provisioning View options.

7 Click OK.

A progress dialog opens showing the progress of the exclude VR command.

If an error occurs while the operation is in progress, a message dialog opens that indicates the error. The operation stops and the tool disconnects from any devices to which it is connected.

Apply is disabled. The status message in the details panel changes to Stored in the server database.

The VR is removed from the VPN. If you selected Exclude VR from VPN and Delete VR, the VR component is also deleted.

Creating a new customer VPN

Creating a customer VPN involves the following procedures:

- “Adding a new customer” (page 80)
- “Adding a new VPN to a customer” (page 82)
- “Adding a VR to a VPN” (page 83)

Chapter 6
Using the IP VPN global update tool CLI

For information on how to use the IP VPN global update tool CLI, see the following sections:

- "Creating a VPN" (page 93)
- "Deleting a VPN" (page 97)
- "Adding a VR to a VPN" (page 97)
- "Excluding a VR from a VPN" (page 98)
- "Adding a policy group to a VR in a VPN" (page 99)
- "Deleting a policy group from a VR in a VPN" (page 101)
- "Configuring a tosMask attribute on a VR" (page 102)
- "Updating a password" (page 103)

Note 1: The following procedures provide command syntax examples.

Note 2: For detailed information on commands, see "Commands" (page 105).

Creating a VPN

When you create a VPN, you must also create the VR component on the Passport switch and include the VR in the VPN.

1 Create a customer and VPN in the database:

```
createvpn vpn1 100 customer1 200 1 system mypassword
```

where:

<vpn1> is the name of the VPN being created.

<100> is the VPN ID.

<customer1> is the customer name.

<200> is the customer ID.

<1> is the autonomous system identifier.

<system> is the userID for the VPN. The userID is used as a default for other commands when no userID is specified.

<mypassword > is the password for the VPN. This password is used as a default for other commands when no password is specified.

2 Create the VR components to include in the VPN:

createvr vpn1 customer1
-vr vpn1 PP1 -vr vpn1 PP2 -vr vpn1 PP3
-save U vpn1_view
-activate

where:

<vpn1> is the name of the VPN you created.

<customer1> is the name of the customer who owns the VPN.

-vr is the VR you are creating.

<PP#> is the Passport on which you are creating the VR. In this example, the VR is being created in three nodes, PP1, PP2, and PP3.

-save saves a specific view.

<U> indicates the provisioning mode. In this example, the mode is user specified.

<vpn1_view> is a complete provisioning file name, which you need to specify if the mode is user specified.

-activate activates the VR.

3 After you create the VRs on each of the nodes, include the new VRs in the VPN.

a. To include the VRs separately:

includevr vpn1 customer1
-vr vpn1 PP1 200.1.1.1 255.255.255.0 100.1.1.1 255.255.255.0 1
-start U vpn1_view
-save U vpn1_view

-activate

includevr vpn1 customer1
-vr vpn1 PP2 200.1.1.2 255.255.255.0 100.1.2.1 255.255.255.0 0
-start U vpn1_view
-save U vpn1_view
-activate

includevr vpn1 customer1
-vr vpn1 PP1 200.1.1.1 255.255.255.0 100.1.1.1 255.255.255.0 1
-start U vpn1_view
-save U vpn1_view
-activate

where:

`<vpn1>` is the VPN name.

`<customer1>` is the name of the customer who owns the VPN.

`-vr` specifies the VR to include in the VPN.

`<PP#>` is the name of the Passport on which the VR exists.

`<200.1.1.1>` is the private IP address of the VR included in PP1.

`<255.255.255.0>` is the network mask of the private IP address for PP1.

`<100.1.1.1>` is the public IP address of the VR included in PP1.

`<255.255.255.0>` is the network mask of the public IP address for PP1.

`<1>` indicates that the VR should be a route reflector. If this VR is set to be a route reflector, all other non-route reflector VRs in the VPN

are set to clients. The number 1 sets the VR to a route reflector, and 0 does not set the VR as a route reflector.

`-start` begins provisioning for a specific view. If you do not specify this parameter, the tool uses the current view.

`[U]` indicates the mode in which to start a provisioning session is user specified.

`<vpn1_view>` is a complete provisioning file name that you specify when the mode is user specified.

`-save` saves a specific view.

`-activate` activates the edit views on all the Passports in the VPN.

b. To include VRs, using a VR file:

includevr vpn1 customer1
-vrfile vrfile.txt
-start U vpn1_view
-save U vpn1_view
-activate

where:

`<vpn1>` is the VPN name

`<customer1>` is the name of the customer who owns the VPN.

`-vrfile` specifies the VR file that contains the list of VRs.

`<vrfile.txt>` is the name of the VR file.

`-start` begins provisioning for a specific view. If you do not specify this parameter, the tool uses the current view.

`[U]` indicates the mode in which to start a provisioning session is user specified.

`<vpn1_view>` is a complete provisioning file name that you specify when the mode is user specified.

`-save` saves a specific view.

`-activate` activates the edit views on all the Passports in the VPN.

VR File Format

The example VR file consists of the following format and information:

```
vpn1 PP1 200.1.1.1 255.255.255.0 100.1.1.1
255.255.255.0 1

vpn1 PP2 200.1.1.2 255.255.255.0 100.1.2.1
255.255.255.0 0

vpn1 PP3 200.1.1.3 255.255.255.0 100.1.3.1
255.255.255.0 0
```

Deleting a VPN

1 Delete the VPN:

deletevpn vpn1 customer1
[-start U vpn1_view]
-save U vpn1_view
-activate

where:

<vpn1> is the name of the VPN that you want to delete.

<customer1> is the name of the customer who owns the VPN.

[-start] begins provisioning for a specific view. If you do not specify this parameter, the tool uses the current view.

<U> indicates the mode in which to start a provisioning session is user specified.

[<viewname>] is a complete provisioning file name, which you specify when the mode is user specified.

-save saves a specific view.

-activate activates the edit views on all the Passports in the VPN.

Adding a VR to a VPN

In this example, the VR vpn1 already exists on the node PP4. If the VR did not exist, you would need to use the createvr command to create it.

1 Add a VR to an existing VPN:

includevr vpn1 customer1
-vr vpn1 PP4 200.1.1.4 255.255.255.0 100.1.4.1 255.255.255.0 0
-start U vpn1_view
-save U vpn1_view
-activate

where:

`<vpn1>` is the VPN name.

`<customer1>` is the name of the customer who owns the VPN.

`-vr` specifies a VR to add to the existing VPN.

`<PP4>` is the name of the Passport on which the VR exists.

`<200.1.1.4>` is the private IP address of the VR.

`<255.255.255.0>` is the network mask of the private IP address for the VR.

`<100.1.4.1>` is the public IP address of the VR.

`<255.255.255.0>` is the network mask of the public IP address of the VR you are adding.

`<0>` indicates the VR is not a route reflector.

`-start` begins provisioning for a specific view. If you do not specify this parameter, the tool uses the current view.

`[U]` indicates the mode in which to start a provisioning session is user specified.

`<vpn1_view>` is a complete provisioning file name that you specify when the mode is user specified.

`-save` saves a specific view.

`-activate` activates the edit views on all the Passports in the VPN.

Excluding a VR from a VPN

This procedure excludes a VR from a VPN. This procedure does not delete the VR component. It only updates the ARP table, tunnel, and border gateway protocol (BGP) information for the VR. If you want to delete the VR component, use the deletevr command.

1 Exclude a VR from an existing VPN:

excludevr vpn1 customer1
-vr vpn1 PP2
-save U test_view
-activate

where:

`<vpn1>` is the VPN name.

`<customer1>` is the name of the customer who owns the VPN.

`-vr` specifies the VR to exclude from the VPN.

`<PP2>` is the name of the Passport on which to exclude the VR.

`-save` saves a specific view.

`[U]` indicates the mode in which to start a provisioning session is user specified.

`<test_view>` is a complete provisioning file name that you specify when the mode is user specified.

`-activate` activates the edit views on all the Passports in the VPN.

Deleting a VR

This procedures deletes a VR from a VPN:

1 Delete the VR

deletevr vpn1 customer1
-vr vpn1 PP2
-save U vpn1_view
-activate

where:

`<vpn1>` is the VPN name.

`<customer1>` is the name of the customer who owns the VPN.

`-vr` specifies the VR to delete from the VPN.

`<PP2>` is the name of the Passport on which to delete the VR.

`-save` saves a specific view.

`[U]` indicates the provisioning mode. In this example, the mode is user specified.

`<vpn1_view>` is a complete provisioning file name, which you need to specify if the mode is user specified.

`-activate` activates the edit views on all the Passports in the VPN.

Adding a policy group to a VR in a VPN

1 Add a policy group to a VR in a VPN:

a. Add a class of service (CoS) policy to all the VRs in a VPN.

addpolicy vpn1 customer1 policy1 pg1 2
-flowClassification 1 10.1.0.0 16 tcp 8080

-save U vpn1_view
-activate

where:

<vpn1> is the VPN that contains the VR to which you are adding the policy.

<customer1> is the name of the customer who owns the VPN.

<policy1> is the name of the policy within the policy group.

<pg1> is the name of the policy group.

<2> is the CoS index.

-flowClassification specifies a flow classification.

<1> specifies the flow class.

<16> is the length of the prefix.

<tcp> specifies the TCP protocol.

<8080> is the port number.

-save saves a specific view.

<U> indicates the mode in which to start a provisioning session is user specified.

<vpn1_view] is a complete provisioning file name that you specify when the mode is user specified.

-activate activates the edit views on all the Passports in the VPN.

b. Add a policy to only one VR in the VPN:

addpolicy vpn1 customer1 policy1 pg1 2
-vr vpn1 PP2
-flowClassification 1 10.1.0.0 16 tcp 8080
-save U vpn1_view
-activate

where:

<vpn1> is the VPN that contains the VR to which you are adding the policy group.

<customer1> is the name of the customer who owns the VPN.

<policy1> is the name of the policy within the policy group.

`<pg1>` is the name of the policy group.

`<2>` is the CoS index consisting.

`-vr` specifies the VR on which to add a policy.

`<PP2>` is the Passport node that contains the VR.

`-flowClassification` specifies a flow classification.

`<1>` specifies the flow class.

`<10.1.0.0>` is the prefix.

`<16>` is the length of the prefix.

`<tcp>` indicates the TCP protocol.

`<8080>` is the port number.

`-save` saves a specific view.

`<U>` indicates the mode in which to start a provisioning session is user specified.

`<vpn1_view]` is a complete provisioning file name that you specify when the mode is user specified.

`-activate` activates the edit views on all the Passports in the VPN.

Deleting a policy group from a VR in a VPN

The example that follows only deletes the flowClassification option from a policy. It does not delete the entire policy.

1 Delete the flowClassification option from a policy:

deletepolicy vpn1 customer1 policy1 pg1 2
-flowClassification 1
-start (U) vpn1_view
-save U vpn1_view
-activate

where:

`<vpn1>` is the VPN that contains the VR from which you are deleting the policy group.

`<customer1>` is the name of the customer who owns the VPN.

`<policy1>` is the name of the policy within the policy group.

<pg1> is the name of the policy group.

<2> is the CoS index.

-flowClassification specifies a flow classification.

<1> specifies the flow class.

-start begins provisioning for a specific view. If you do not specify this parameter, the tool uses the current view.

<U> indicates the mode in which to start a provisioning session is user specified.

<vpn1_view] is a complete provisioning file name that you specify when the mode is user specified.

-save saves a specific view.

-activate activates the edit views on all the Passports in the VPN.

Configuring a tosMask attribute on a VR

1 Configure a type of service (TOS) mask attribute on a VR in a VPN:

settosmask vpn1 customer1 policy1tosMask
-start U vpn1_view
-save U vpn1_view
[-activate]

where:

<vpn1> is the VPN that contains the VR for which you are configuring the tosMask attribute.

<customer1> is the name of the customer who owns the VPN.

<policy1> is the name of the policy within the policy group.

[<tos_mask>] is the ToS mask value.

-vr specifies the VR.

<vr1> is the VR in the policy group.

-start begins provisioning for a specific view. If you do not specify this parameter, the tool uses the current view.

<U> indicates the mode in which to start a provisioning session is user specified.

<vpn1_view> is a complete provisioning file name, which you specify when the mode is user specified.

`-save` saves a specific view.

`-activate` activates the edit views on all the Passports in the VPN.

Updating a password

This procedure updates the default passwords for all Passport nodes in the VPN.

1 Update the default password.

updatepasswd vpn1 customer1 system mypasswd -default

where:

`<vpn1>` is the VPN name.

`<customer1>` is the name of the customer who owns the VPN.

`<system>` is the userID to log in to the Passports.

`<mypasswd>` is the password for the userID.

`-default` indicates that you are updating all the default userIDs and passwords for all Passport nodes in the VPN.

Chapter 7
Commands

For a description of the commands for the IP VPN global update tool, see the following sections:

- “help” (page 105)
- “createvpn” (page 106)
- “createvr” (page 107)
- “includevr” (page 108)
- “excludevr” (page 111)
- “deletevr” (page 113)
- “deletevpn” (page 115)
- “settosmask” (page 116)
- “settosmarking” (page 118)
- “addpolicy” (page 120)
- “deletepolicy” (page 122)
- “listvpn” (page 124)
- “listcustomer” (page 125)
- “updatepasswd” (page 125)

help

Use the help option to obtain help on the commands and options listed in this section.

The command syntax for the help command is as follows:

```
<command> -help
```

where:

<command> is the command you want to obtain help for.

An example of the help command follows:

```
createvpn -help
```

createvpn

Use the createvpn command to initialize the database tables for the VPN that you are creating. The createvpn command does not perform any provisioning commands on the Passport nodes.

The command syntax for the createvpn command is as follows:

```
createvpn <vpn> <vpn_id> <customer> <customer_id> /
<as_id>
[<userid> <passwd>]
[-auto]
[-log <logfile>]
[-help]
```

where:

<vpn> is the name of the VPN you want to create.

<vpn_id> is the unique identifier for the VPN.

<customer> is the name of the customer who will own the VPN.

<customer_id> is the unique ID of the customer.

<as_id> is the autonomous system identifier.

[<userid><passwd>] where <userid> is a default userid that you can use to log into all Passport nodes in the VPN and <passwd> is a default password for the userid.

[-auto] is the option to specify auto discovery mode.

[-log <logfile>] is the option to specify a log file. If you specify the log file, logging is turned on. If you do not specify the log file, a default log file is used. <logfile> is the name of the log file

[-help] displays help for the command.

An example of the createvpn command follows:

```
createvpn vpnABC 101 custABC 201 1
```

createvr

Use the createvr command to create a VR component.

The command syntax for the createvr command is as follows:

```
createvr <vpn> <customer>
-vr <vr> <pp> [<userid> <passwd>]]
[-start<mode> [<key> | <date> | <viewname>]]
-save<mode> [<key> | <date> | <viewname>]
[-activate]
[-commit]
[-log <logfile>]
[-help]
```

where:

<vpn> is the VPN name.

<customer> is the name of the customer who will own the VPN.

-vr is the VR you are creating. You can specify more than one VR.

<vr> is the name of the VR being created.

<pp> is the Passport on which you are creating the VR.

[<userid>] is the userID to log in to the Passport switch.

[<passwd>] is the password for the userID.

`[-start]` indicates provisioning will start for a specific view.

`[<mode>]` applies to the start and save options. For the start option, select one of: USER_SPECIFIED (U), KEYED (K), DATED (D), CURRENT (CUR), or COMMITED (COM). For the save option, select one of USER_SPECIFIED (U), KEYED (K), or DATED. (KEYED and DATED are not supported in this release.)

`[<key>]` is composed of letters, digits, and underscores. A key cannot begin with an underscore or exceed more than six characters.

`[<date>]` is the valid date (specified as YYMMDD).

`[<viewname>]` is a complete provisioning file name. Use this parameter when the mode is USER_SPECIFIED.

`-save` saves a specific view.

`[-activate]` activates the VR.

`[-commit]` commits the VR.

`[-log <-logfile>]` specifies the name of the log file. If you specify the log file, logging is turned on.

`[-help]` displays help for the command.

An example of the createvr command follows:

```
createvr vpnABC custABC
-vr A PP1
-save USER_SPECIFIED vpnview_abc
-activate
-commit
```

includevr

Use the includevr command to include a VR in the VPN. You can include each VR separately or use a VR file that contains the VRs. (The includevr command assumes that the VR component currently exists.) The includevr command updates all tunnels in the VPN to take into account all the newly included VRs, as well as updating all ARP tables of all VRs in the VPN.

The includevr command also updates the VR related information in the IP VPN database.

The command syntax for the includevr command is as follows:

```
includevr <vpn> <customer>
-vr <vr> <pp> <private_ip> <private_netmask>
<public_ip> <public_netmask> <isroutereflector>
[<topology>] [<userid> <passwd>]
[-vr <vr> <pp> <private_ip> <private_netmask>
<public_ip> <public_netmask> <isroutereflector>
[<topology>] [<userid> <passwd>]]

[-vr_file <vrfile>]
[-db]
[-start<mode> [<key> | <date> | <viewname>]]
-save <mode> [<key> | <date> | <viewname>]
[-activate]
[-commit]
[-log <logfile>]
[-help]
```

where:

`<vpn>` is the VPN name.

`<customer>` is the name of the customer who owns the VPN.

`-vr` specifies a VR to be included in the VPN. You can specify more than one VR in the includevr command.

`<vr>` the name of the VR you are including.

`<pp>` is the name of the Passport on which the VR exists.

`<private_ip>` is the private IP address of the VR.

`<private_netmask>` is the network mask of the private IP address.

`<public_ip>` is the public IP address of the VR.

`<public_netmask>` is the network mask of the public IP address.

`<isroutereflector>` indicates whether or not the VR should be a route reflector. If the VR is set to be a route reflector, all other non-route reflector VRs in the VPN are set to clients. If the IS_ROUTE_REFLECTOR parameter is 1, the VR is set to be a route reflector, and the BGP peerage is updated. If the IS_ROUTE_REFLECTOR parameter is 0, the VR is not set to be a route reflector.

`[<topology>]` is the option to specify either a hub or spoke. If the VPN was created in auto discovery mode, the default value is hub.

The VR is assumed to be spoke if:

- the auto option was specified in the createvpn command, and
- the hub and isroutereflector options are not specified in the includevr command

`[<userid>]` is the userID to log in to the Passport switch.

`[<passwd>]` is the password for the userID.

`[-vr_file]` allows you to read in the VRs to be included in the VPN through an ASCII text file. This file contains a list of the VRs with their public and private IP addresses and network masks.

`[<vrfile>]` is the name of the VR file which contains a list of VRs to be included in the VPN.

`[-db]` updates the database, but does not perform any provisioning on the switches. This option is useful if you have already provisioned the VRs, and only want to update the database.

`[-start]` begins provisioning for a specific view. If you do not specify this parameter, the tool uses the current view.

`[<mode>]` applies to the start and save options. For the start option, select one of: USER_SPECIFIED (U), KEYED (K), DATED (D), CURRENT (CUR), or COMMITED (COM). For the save option, select one of USER_SPECIFIED (U), KEYED (K), or DATED. (KEYED and DATED are not supported in this release.)

`[<key>]` is composed of letters, digits, and underscores. A key cannot begin with an underscore or exceed more than six characters.

`[<date>]` is the valid date (specified as YYMMDD).

`[<viewname>]` is a complete provisioning file name. Use this parameter when the mode is USER_SPECIFIED.

`-save` saves a specific view.

`[-activate]` activates the edit views on all the Passports in the VPN.

`[-commit]` commits the views on all the Passports in the VPN.

`[-log <logfile>]` specifies the name of the log file. If you specify the log file, logging is turned on.

`[-help]` displays help for the command.

An example of the includevr command follows:

```
includevr vpnABC custABC
-vr D PP3 200.1.1.4 255.255.255.0 40.1.1.1 255.0.0.0 0
-start USER_SPECIFIED vpnview_abc
-save USER_SPECIFIED vpnview_abc
-activate
```

excludevr

Use the excludevr command to remove a VR from a VPN. The command deletes any related entries from the IP VPN database. It also updates the tunnels of all the VRs in the VPN, as well as the ARP tables of the VRs. The command syntax for the excludevr command is as follows:

```
excludevr <vpn> <customer>
-vr <vr> <pp>
[-vr <vr> <pp>]
[-vr_file <vrfile>]
[-db]
[-start <mode> [<key> | <date> | <viewname>]]
-save <mode> [ <key> | <date> | <viewname>]
[-activate]
```

```
[-commit]
[-log <logfile>]
[-help]
```

where:

`<vpn>` is the VPN name.

`<customer>` is the name of the customer who owns the VPN.

`-vr` specifies a VR to be excluded from the VPN. You can specify more than one VR in the excludevr command.

`<vr>` is the name of the VR that you are excluding.

`<pp>` is the name of the Passport on which the VR exists.

`[-vr_file]` lets you read in the VRs to be excluded from the VPN through an ASCII text file. This file contains a list of the VRs with their public and private IP addresses and network masks.

`[<vrfile>]` is the name of the VR file which contains a list of VRs to be excluded from the VPN.

`[-db]` updates the database, but does not perform any provisioning on the switches. This option is useful if you have already provisioned the VRs, and only want to update the database.

`[-start]` begins provisioning for a specific view. If you do not specify this parameter, the tool uses the current view.

`[<mode>]` applies to the start and save options. For the start option, select one of: USER_SPECIFIED (U), KEYED (K), DATED (D), CURRENT (CUR), or COMMITED (COM). For the save option, select one of USER_SPECIFIED (U), KEYED (K), or DATED. (KEYED and DATED are not supported in this release.)

`[<key>]` is composed of letters, digits, and underscores. A key cannot begin with an underscore or exceed more than six characters.

`[<date>]` is the valid date (specified as YYMMDD).

`[<viewname>]` is a complete provisioning file name. Use this parameter when the mode is USER_SPECIFIED.

`-save` saves a specific view.

`[-activate]` activates the edit views on all the Passports in the VPN.

`[-commit]` commits the views on all the Passports in the VPN.

`[-log <logfile>]` specifies the name of the log file. If you specify the log file, logging is turned on.

`[-help]` displays help for the command.

An example of the excludevr command follows:

```
excludevr vpnABC custABC
-vr B PP2
-vr C PP3
-activate
-save
```

deletevr

The deletevr command lets you specify the VRs to be deleted from a VPN in a Passport node.

The command syntax for the deletevr command is as follows:

```
deletevr <vpn> <customer> -vr <vr> <pp> [<userid>
<passwd>]
[-vr <vr> <pp> [<userid> <passwd>]...
[-start <mode> [<viewname>]]
-save <mode> <viewname>
[-activate]
[-commit]
[-log <logfile>]
[-help]
```

where:

<vpn> is the name of the VPN for which the vr(s) are being deleted.

<customer> is the name of the customer who owns the VPN.

-vr This option is used to specify a vr to be deleted.

<vr> The name of the vr to be deleted.

<pp> The name of the passport node from which the vr will be deleted.

<userid> The user ID used to login to the passport node.

<passwd> The password for the above user ID.

[-start] The start option is used to specify the view to be used when entering provisioning on the passport nodes in the VPN.

[<mode>] applies to the view option for the start option. Select one of: CURRENT (CUR), EDIT (E), COMMITED (COM), USER_SPECIFIED (U), DATED (D), KEYED (K). For USER_SPECIFIED, DATED, or KEYED, the user also has to specify a viewname or a date or a key depending on the option.

Note: DATED and KEYED are not implemented in this release.

[<key>] is composed of letters, digits, and underscores. A key cannot begin with an underscore or exceed more than six characters.

[<date>] is the valid date (specified as YYMMDD).

[<viewname>] is a complete provisioning file name. Use this parameter when the mode is USER_SPECIFIED.

-save The save option is used to specify a specific view to save any provisioning changes on the passport nodes in the VPN. The view <mode> can be one of the following: USER_SPECIFIED (U), DATED (D), or KEYED (K).

[-activate] The activate option indicates that the provisioning view on any affected Passport nodes in the VPN should be activated after the command has successfully completed.

[-commit] The commit option indicates that the provisioning view on any affected Passport nodes in the VPN should be committed after the command has successfully completed.

[-log <logfile>] specifies the name of the log file. If you specify the log file, logging is turned on. The log file is specified by the <logfile> parameter. <logfile> should contain the full directory path.

[-help] displays help for the command.

deletevpn

The deletevpn command first performs an excludevr command on all the VRs in the VPN and then excludes the VPN from the database.

The command syntax for the deletevpn command is as follows:

```
deletevpn <vpn> <customer>
[-start <mode> [<key> | <date | <viewname>]]
-save <mode> [ <key> | <date>|<viewname>]
[-activate]
[-commit]
[-log <logfile>]
[-help]
```

where:

<vpn> is the VPN name.

<customer> is the name of the customer who owns the VPN.

[-start] begins provisioning for a specific view. If you do not specify this parameter, the tool uses the current view.

`[<mode>]` applies to the start and save options. For the start option, select one of: USER_SPECIFIED (U), KEYED (K), DATED (D), CURRENT (CUR), or COMMITED (COM). For the save option, select one of USER_SPECIFIED (U), KEYED (K), or DATED. (KEYED and DATED are not, however, supported in this release.)

`[<key>]` is composed of letters, digits, and underscores. A key cannot begin with an underscore or exceed more than six characters.

`[<date>]` is the valid date (specified as YYMMDD).

`[<viewname>]` is a complete provisioning file name. Use this parameter when the mode is USER_SPECIFIED.

`-save` saves a specific view.

`[-activate]` activates the edit views on all the Passports in the VPN.

`[-commit]` commits the views on all the Passports in the VPN.

`[-log <logfile>]` specifies the name of the log file. If you specify the log file, logging is turned on.

`[-help]` displays help for the command.

An example of the deletevpn command follows:

```
deletevpn vpnABC custABC
-save USER_SPECIFIED vpnview_abc
-activate
-commit
```

settosmask

Use the settomask command to set up a type of service (ToS) mask for a class of service (CoS) treatment component.

The command syntax for the settosmask command is as follows:

`settosmask <vpn> <customer> <policygroup> <tosMask>`

```
[-vr <vr> <pp>
[-start<mode> [<key> | <date> | <viewname>]]
-save <mode> [<key> | <date> | <viewname>]
[-activate]
[-commit]
[-log <logfile>]
[-help]
```

where:

`<vpn>` is the VPN name. The policy is added to all the VRs in this VPN.

`<customer>` is the name of the customer who owns the VPN.

`<policygroup>` is the name of the policy group (consisting of a 20-character string) that defines a common set of policies.

`<tosMask>` is a ToS mask value.

`[-vr]` specifies a list of VRs on which to perform this command.

`[<vr>]` is the name of the VR.

`[<pp>]` is the name of the Passport on which the VR exists.

`[-start]` begins provisioning for a specific view. If you do not specify this parameter, the tool uses the current view.

`[<mode>]` applies to the start and save options. For the start option, select one of: USER_SPECIFIED (U), KEYED (K), DATED (D), CURRENT (CUR), or COMMITED (COM). For the save option, select one of USER_SPECIFIED (U), KEYED (K), or DATED. (KEYED and DATED are not supported in this release.)

`[<key>]` is composed of letters, digits, and underscores. A key cannot begin with an underscore or exceed more than six characters.

`[<date>]` is the valid date (specified as YYMMDD).

`[<viewname>]` is a complete provisioning file name. Use this parameter when the mode is USER_SPECIFIED.

`-save` saves a specific view.

`[-activate]` activates the edit views on all the Passports in the VPN.

`[-commit]` commits the views on all the Passports in the VPN.

`[-log <logfile>]` specifies the name of the log file. If you specify the log file, logging is turned on.

`-help` displays help for the command.

An example of the settosmask command follows:

```
settosmask vpnABC custABC pg12 2
-save USERSPECIFIED vpnview_abc
-activate
-commit
```

settosmarking

Use the settosmarking command to set up a ToS setting for a CoS treatment component.

The command syntax for the settosmarking command is as follows:

```
settosmarking <vpn> <customer> <policygroup>

[-vr <vr> <pp>]
-setToS <cos_treatment> <tos>
[-setToS <cos_treatment> <tos>]
[-off <cos_treatment>]
[-on <cos_treatment>]
[-start <mode> [<key> | <date> | <viewname]]
-save <mode> [ <key> | <date> | <viewname>]
[-activate]
[-commit]
[-log<logfile>]
[-help]
```

where:

`<vpn>` is the VPN name. The policy is added to all the VRs in this VPN.

`<customer>` is the name of the customer who owns the VPN.

<policygroup> is the name of the policy group (consisting of a 20-character string) that defines a common set of policies.

[-vr] specifies a list of VRs on which to perform this command.

<vr> is the VR name.

[<pp>] is the name of the Passport on which the VR exists.

-setToS specifies a ToS setting.

<cos_treatment> is an integer (between 1 and 4) that represents the CoS treatment index.

<tos> is a ToS value.

[-off] turns off the set ToS marking if this flag is present.

[-on] turns on the set ToS marking if this flag is present.

[-start] begins provisioning for a specific view. If you do not specify this parameter, the tool uses the current view.

[<mode>] applies to the start and save options. For the start option, select one of: USER_SPECIFIED (U), KEYED (K), DATED (D), CURRENT (CUR), or COMMITED (COM). For the save option, select one of USER_SPECIFIED (U), KEYED (K), or DATED. (KEYED and DATED are not supported in this release.)

[<key>] is composed of letters, digits, and underscores. A key cannot begin with an underscore or exceed more than six characters.

[<date>] is the valid date (specified as YYMMDD).

[<viewname>] is a complete provisioning file name. Use this parameter when the mode is USER_SPECIFIED.

-save saves a specific view.

[-activate] activates the edit views on all the Passports in the VPN.

[-commit] commits the views on all the Passports in the VPN.

[-log <logfile>] specifies the name of the log file. If you specify the log file, logging is turned on.

-help displays help for the command.

An example of the settosmarking command follows:

```
settosmarking vpnABC custABC pg12
-setToS 1 3
-off 1
-save USER_SPECIFIED vpnview_abc
-activate
-commit
```

addpolicy

Use the addpolicy command to add a flow classification or ToSMap to a policy. If the policy does not exist, it is created.

The command syntax for the addpolicy command is as follows:

```
addpolicy <vpn> <customer> <policyname> <policygroup>
[<cos_index>]
[-vr <vr> <pp]
[-tosMap <tos>...]
[-flowClassification <flowclass_id> <prefix>
<prefixLength> <protocol> <port>]
[-start<mode> [<key> | <date> | <viewname>]]
-save <mode> [<key> | <date> | <viewname>]
[-activate]
[-commit]
[-log<logfile>]
[-help]
```

where:

<vpn> is the VPN name.

<customer> is the name of the customer who owns the VPN.

<policyname> is the name of the policy within the policy group.

`<policygroup>` is the name of the policy group (consisting of a 20-character string) that defines a common set of policies.

`[<cos_index>]` is the CoS index (consisting of a value of 0, 1, 2, or 3).

`[-vr]` specifies a list of VRs on which to perform this command. If you do not use this option, the policy is added to all VRs in the VPN.

`[<vr>]` is the VR in the policy group that you are adding.

`[<pp>]` is the name of the Passport.

`[-tosMap]` specifies a ToS setting.

`[<tos>]` specifies a ToS value.

`[-flowClassification>]` specifies a flow classification.

`[-flowclass_id>]` specifies the flow classification identifier.

`[<prefix>]` specifies the prefix for the flow classification.

`[<prefixLength>]` is the length of the prefix.

`[<protocol>]` is the protocol (either TCP, UDP, or ICMP).

`[<port>]` specifies the port number.

`[-start]` begins provisioning for a specific view. If you do not specify this parameter, the tool uses the current view.

`[<mode>]` applies to the start and save options. For the start option, select one of: USER_SPECIFIED (U), KEYED (K), DATED (D), CURRENT (CUR), or COMMITED (COM). For the save option, select one of USER_SPECIFIED (U), KEYED (K), or DATED. (KEYED and DATED are not supported in this release.)

`[<key>]` is composed of letters, digits, and underscores. A key cannot begin with an underscore or exceed more than six characters.

`[<date>]` is the valid date (specified as YYMMDD).

`[<viewname>]` is a complete provisioning file name. Use this parameter when the mode is USER_SPECIFIED.

`-save` saves a specific view.

`[-activate]` activates the edit views on all the Passports in the VPN.

`[-commit]` commits the views on all the Passports in the VPN.

`[-log <logfile>]` specifies the name of the log file. If you specify the log file, logging is turned on.

`[-help]` displays help for the command.

An example of the addpolicy command follows:

```
addpolicy vpnABC custABC policy1 pg12
-flowClassification 1 10.1.0.0 16 tcp 8080
-activate
-save
```

deletepolicy

Use the deletepolicy command to delete a policy for a VR.

The command syntax for the deletepolicy command is as follows:

```
deletepolicy <vpn> <customer> <policyname>
<policygroup>
[-vr <vr> <pp]
[-tosMap]
[-flowClassification <flowclass>]
[-start<mode> [<key> | <date> |<viewname>]]
-save<mode> [<key> | <date> | <viewname>]
[-activate]
[-commit]
[-log<logfile>]
[-help]
```

where:

<vpn> is the VPN name. The policy is added to all the VRs in this VPN.

<customer> is the name of the customer who owns the VPN.

<policyname> is the name of the policy within the policy group.

<policygroup> is the name of the policy group (consisting of a 20-character string) that defines a common set of policies.

[-vr] specifies a list of VRs from which to delete a policy.

[<vr>] is the name of the VR from which the policy is being deleted.

[<pp>] is the name of the Passport.

[-tosMap] deletes the ToS map. If you do not specify this option, the entire policy is deleted from the specified VRs.

[-flowClassification] deletes the specified flow classification from the policy. If you do not specify this option, the entire policy is deleted.

[<flowclass>] is the flow classification you wish to delete.

[-start] begins provisioning for a specific view. If you do not specify this parameter, the tool uses the current view.

[<mode>] applies to the start and save options. For the start option, select one of: USER_SPECIFIED (U), KEYED (K), DATED (D), CURRENT (CUR), or COMMITED (COM). For the save option, select one of USER_SPECIFIED (U), KEYED (K), or DATED. (KEYED and DATED are not supported in this release.)

[<key>] is composed of letters, digits, and underscores. A key cannot begin with an underscore or exceed more than six characters.

[<date>] is the valid date (specified as YYMMDD).

[<viewname>] is a complete provisioning file name. Use this parameter when the mode is USER_SPECIFIED.

`-save` saves a specific view.

`[-activate]` activates the edit views on all the Passports in the VPN.

`[-commit]` commits the views on all the Passports in the VPN.

`[-log <logfile>]` specifies the name of the log file. If you specify the log file, logging is turned on.

`[-help]` displays help for the command.

An example of the deletepolicy command follows:

```
deletepolicy vpnABC custABC policy1 pg12
-flowClassification 1 tcp 8080
-activate
-save
```

listvpn

Use the listvpn command to list the VPNs in the Passport network.

The command syntax for the listvpn command is as follows:

```
listvpn <vpn> <customer>
[-vr]
[-pp]
[-vpn_id]
[-log<logfile>]
[-help]
```

where:

`<vpn>` is the VPN name.

`<customer>` is the name of the customer who owns the VPN.

`[-vr]` displays the VRs included in the VPN.

`[-pp]` displays the Passport nodes in the VPN.

`[-vpn_id]` displays the ID of the VPN.

[-log <logfile>] specifies the name of the log file. If you specify the log file, logging is turned on.

[-help] displays help for the command.

An example of the listvpn command follows:

```
listvpn vpnABC custABC
-vr
```

listcustomer

Use the listcustomer command to list the VPNs for a specific customer.

The command syntax for the listcustomer command is as follows:

```
listcustomer <customer> <-vpn | -customer_id>
[-log<logfile>]
[-help]
```

where:

<customer> is the name of the customer who owns the VPN.

<-vpn | -customer_id> where -vpn displays the VPNs owned by the customer and -customer_id displays the ID of the customer.

[-log <logfile>] specifies the name of the log file. If you specify the log file, logging is turned on.

[-help] displays help for the command.

An example of the listcustomer command follows:

```
listcustomer custABC
-vpn
```

updatepasswd

Use the updatepasswd command to update your userID or password for logging into a Passport node.

The command syntax for the updatepasswd command is as follows:

```
updatepasswd <vpn> <customer> <userid> <passwd>
[-pp <pp>]
[-default]
[-log<logfile>]
[-help]
```

where:

`<vpn>` is the VPN name.

`<customer>` is the name of the customer who owns the VPN.

`<userid>` is the userID to log in to the Passport.

`<passwd>` is the password for the userID.

`[-pp]` updates only the userID and password for the named Passport node. If this option is not used, all the nodes in the VPN are updated.

`[<pp>]` is the Passport for which the userID is being set.

`-default` updates only the default userID and password for all the Passport nodes in the VPN.

`[-log <logfile>]` specifies the name of the log file. If you specify the log file, logging is turned on.

`[-help]` displays help for the command.

An example of the updatepasswd command follows:

```
updatepasswd vpnABC custABC
```

Index

A

Add Flow Classification dialog
  about 71
Add New CoS Policy dialog 67
  about 66
adding a flow classification to a policy 88
adding a new customer 80
adding a new VPN to a customer 82
adding a policy 87
adding a VR to an existing VPN 83
addpolicy 120
applying IP CoS to a VPN 86
  procedures
    adding a flow classification 88
    adding a policy 87
    deleting a policy 88
    modifying a flow classification 89
    modifying a policy 87
    opening the Edit Class of Service dialog 86
    provisioning the CoS policy group 86
architecture 18
ARP tables 16
auto discovery 48
  about 17, 50
auto discovery and route reflector 51

C

configuring the end-to-end server 24
configuring the IP VPN global server 25
Confirm Provisioning Options dialog 60, 80
  about 59
  saving provisioning data 61
  selecting a device view 60
CoS policy group
  provisioning 86
CoS Policy Group dialog 64
  about 63
createvpn 106
createvr 107
creating a new customer VPN 91
Creating a VPN 93
customer
  removing a VPN from 85
customer details 44, 45
  valid values and ranges 46
customer selected menu 41
  procedures 81
    adding a new VPN to a customer 82
    removing a customer from the service provider 81
customer VPN
  creating 91

D

database
  location 18, 24
deletepolicy 122
deletevpn 115
deletevr 113

deleting a policy 88
deleting a VPN 97
deleting a VR from an existing VPN 90
details panel 43
  customer details 44
  VPN details 46
  VR details 51
dialogs 55
  Add Flow Classification dialog 71
  Add New CoS Policy dialog 66
  Confirm Provisioning Options dialog 59
  CoS Policy Group dialog 63
  error dialogs 76
  Exclude VR dialog 75
  Include VR dialog 62
  message dialogs 76
  Modify CoS Policy dialog 69
  Modify Flow Classification dialog 73
  Options dialog 56, 57
  Progress dialogs 77

E

Edit Class of Service dialog
  opening 86
end-to-end server 18, 20, 24
error dialogs 76
Exclude VR dialog
  about 75
excludevr 111
excluding a VR from an existing VPN 90

F

flow classification
  adding 89
  adding to a policy 88

H

hierarchy panel 43
hub 51, 55

I

Include VR dialog
  about 62
includevr 108
installing
  license key 34
IP tunneling 16
IP VPN database 18, 20
IP VPN global server 18, 25
IP VPN global update command line 18, 20
IP VPN global update tool
  dialogs 55
IP VPN global update tool CLI
  using 93
IP VPN global update tool GUI 37
  main window 37
IP VPN global update tool main window
  details panel 43
  hierarchy panel 43
IPCoS
  provisioning 63

L

license key 34
limitations 21
listcustomer 125
listvpn 124
log files
  location 23

M

messsage dialogs 76
Modify CoS Policy dialog
  about 69
Modify Flow Classification dialog
  about 73
modifying a flow classification 89
modifying a policy 87

O

opening the Edit Class of Service dialog 86

Options dialog 57
about 56
and Confirm Provisioning dialog 56
saving provisioning data 58
selecting a device view 57
overview 15

P

password, updating 103
policy group
adding for a VR in a VPN 99
deleting from a VR in a VPN 101
procedure 81
procedures
adding a flow classification 88, 89
adding a new VPN to a customer 82
adding a policy 87
adding a VR to an existing VPN 83
applying IP CoS to a VPN 86
applying or changing IP CoS for a VPN 86
customer selected menu
procedures 81
deleting a policy 88
deleting a VR from an existing VPN 90
excluding a VR from an existing VPN 90
modifying a policy 87
opening the Edit Class of Service dialog 86
provisioning the CoS policy group 86
removing a VPN from a customer 85
saving provisioning data 79
seleting a device view 79
VPN selected menu procedures 83
Progress dialogs
about 77
provisioning the CoS policy group 86
public IP aggregation 51

R

removing a customer from the service provider 81
removing a VPN from a customer 85
restrictions 21
route reflector 16, 51, 55

S

saving provisioning data 79
selected menu 40
customer selected menu 41
service provider selected menu 41
VPN selected menu 41
VR selected menu 42
selecting a device view 79
server options 23
servers 24
service provider
removing a customer 81
Service provider selected menu
adding a new customer 80
procedures 80
service provider selected menu 41
settosmarking 118
settosmask 116
spoke 51, 55
starting the IP VPN global update tool 31

T

tooltips 44
tosMask
adding to a VR 102

U

updatepasswd 125
updating a password 103

V

virtual router
adding to a VPN 97
excluding from a VPN 98
VPN
adding a policy group for a VR 99
adding a VR 97
configuring a tosMask attribute on a

VR 102
creating 93
deleting 97
deleting a policy group from a VR 101
excluding a VR 98
VPN details 46, 47
valid values and ranges 48
VPN identifier 48
VPN selected menu 41
procedures 83
adding a VR to an existing VPN 83
applying IP CoS to a VPN 86
removing a VPN from a customer 85
VR details 51, 53
public IP aggregation 51
VR selected menu 42
procedures 90
deleting a VR from an existing VPN 90
excluding a VR from an existing VPN 90

Preside Multiservice Data Manager

Service Provisioning for IP VPN Global Update

User Guide

Release: R14.3RSUP

Publication: 241-6001-601
Document status: Standard
Document version: 14.3RSUP
Document date: December 2003
Printed in Canada