NORTEL NETWORKS

Preside MDM

IP VPN Service Configuration

241-6001-616

Preside MDM

IP VPN Service Configuration

User Guide

Publication: 241-6001-616
Document status: Standard
Document version: 15.1RSUP
Document date: August 2004

Printed in Canada

Publication history

August 2004

15.1 RSUP Standard
Commercial availability except for MPE support which will be available in a future release.

Contents

About this document

This document describes how to use the:

- IP VPN Service Provisioning tool to configure RFC 2547 VPNs and RFC 2764 VPNs with autodiscovery enabled.
- IP VPN Provider Edge Provisioning tool to configure the BGP peers in a provider edge (PE) network. This is required so that you can configure RFC 2547 IP VPN service

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 13)
- "Related documents" (page 14)
- "How to get more help" (page 14)

Who should read this document and why

This document is intended for personnel who are responsible for configuring RFC 2547 VPN service or 2764 VPNs with autodiscovery enabled.

MDM IP VPN Service Configuration tools

This is a new document in the Preside Multiservice Data Manager (MDM) suite. Two new MDM features are described in this document:

- The IP VPN Service Provisioning feature introduces a new user interface and provisioning tool to provision RFC 2547 VPNs and RFC 2764 Autodiscovery mode VPNs.
- The IP VPN Provider Edge Provisioning feature introduces a new user interface and provisioning tool to provision new BGP peers for a Provider Edge network offering RFC 2547 VPN service.

What you need to know

You need to be familiar with the Nortel Networks product, Preside Multiservice Data Manager, and IP VPN architecture and concepts.

How this document is organized

This document contains the following sections:

- “BGP peering configuration” (page 15)
- “2547 IP VPN configuration” (page 27)
- “2764 autodiscovered VPN configuration” (page 49)
- “Administering VPNs” (page 63)
- “IP VPN service provisioning tool” (page 83)
- “IP VPN provider edge provisioning tool” (page 111)

What’s new in this document

This document has been updated to include the following feature:

- “VPN Access Provisioning” (page 12)

VPN Access Provisioning

This feature includes the following enhancements:

- For 2547 IP VPNs, the IP VPN SP tool allows the user to configure the Local ATM access to the customer site

- The IP VPN SP tool allows the user to provision the VRF access details using the IP VPN SP GUI without launching the Embedded Nodal Provisioning tool.

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

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

  Passport commands are not case-sensitive and do not have to match commands and parameters exactly as shown in this document, with the exception of string options values (for example, file and directory names) and string attribute values.

- |

  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:

- NN10600-582 *Passport 7400, 15000, 20000 VPN Configuration Management*
- 241-6001-400 *Preside MDM Administration Database User Guide*

Chapter 1
BGP peering configuration

Use the IP VPN Provider Edge Provisioning (PEP) tool to configure the BGP peers in a PE (Provider Edge) network. BGP peering is required for the configuration of RFC 2547 IP VPNs.

If you have used other methods to configure the BGP peers in your PE network, you can discover them and then use the IP VPN PEP tool to administer and modify them as follows:

- adding/removing peering relationships in a fully peered mesh network
- adding/removing Passport routers in a route reflector network.

For information about the discovery process and how to set up the PE network before you use the IP VPN PEP tool to administer existing BGP peers, see 241-6001-400 *Preside MDM Administration Database User Guide*.

ATTENTION	If an existing PE Network has BGP peers that have been provisioned using other methods, you must use the Preside Multiservice Data Manager Database Administration tool to add them to the PE Network in the Administration Database. See 241-6001-400 *Preside MDM Administration Database User Guide*, Adding core routers to a Provider Edge Network.

This document contains the following sections:

- “Prerequisites to BGP peering configuration”
- “BGP peering configuration procedures”

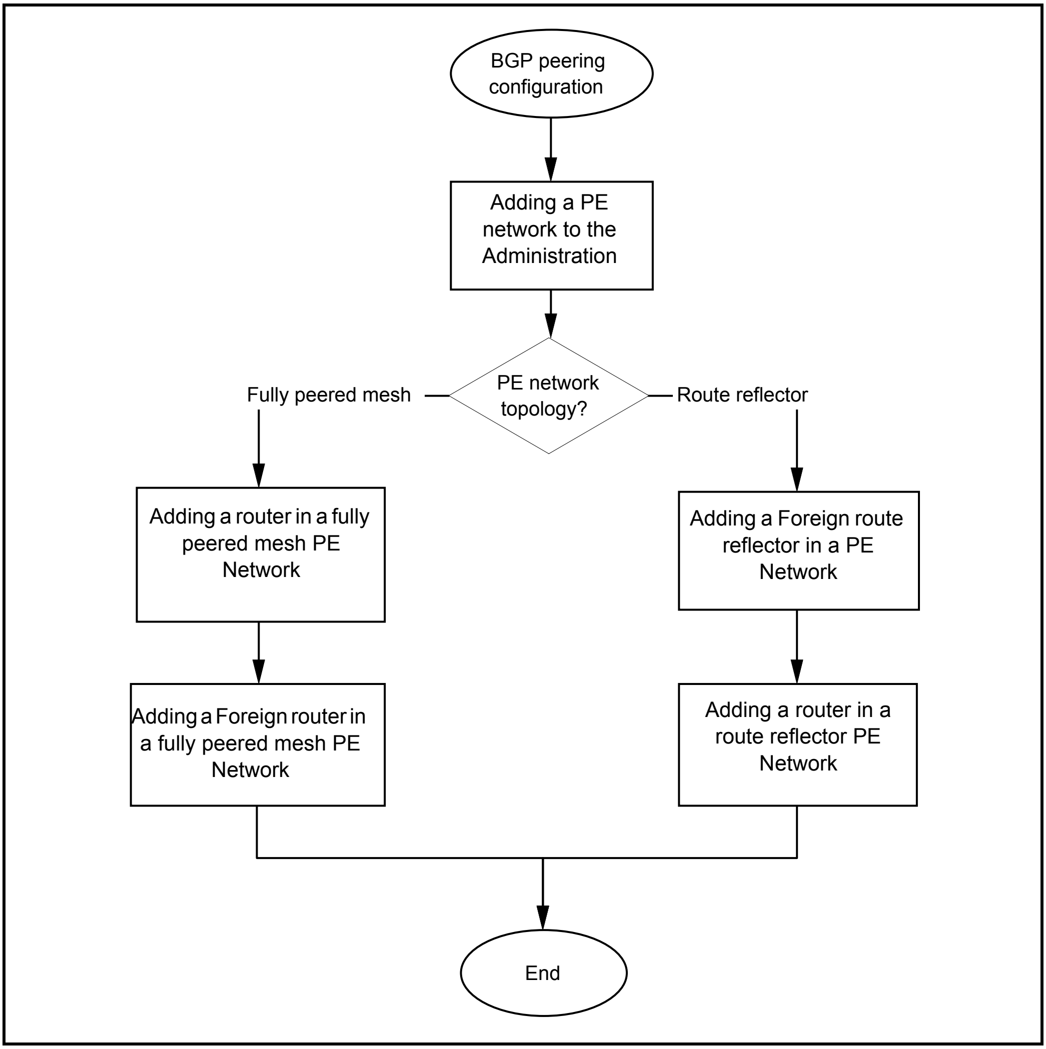
Prerequisites to BGP peering configuration

- Configure the MPLS backbone between the provider edge (PE) nodes. See NN10600-582 *Passport 7400, 15000, 20000 VPN Configuration Management* for the following procedure:
  - *Configuring the PE node backbone for BGP/MPLS VPN*
- Install and configure the Preside Multiservice Data Manager Administration Database to support VPNs. See 241-6001-400 *Preside MDM Administration Database User Guide*.
- Install and configure the physical interfaces between the PE nodes.

BGP peering configuration procedures

The task flow shows you the sequence of procedures you perform to configure BGP peering in a PE network. To link to any procedure in this document, double-click on the procedure name in the task flow or in the "BGP peering configuration procedure navigation" list.

Figure 1
2547 VPN configuration procedures


BGP peering configuration
Adding a PE network to the Administration
PE network topology?
Fully peered mesh
Route reflector
Adding a router in a fully peered mesh PE Network
Adding a Foreign router in a fully peered mesh PE Network
Adding a Foreign route reflector in a PE Network
Adding a router in a route reflector PE Network
End

BGP peering configuration procedure navigation

- "Adding a PE network to the Administration Database"
- "Adding a router in a fully peered mesh PE Network"
- "Adding a Foreign router in a fully peered mesh PE Network"

- “Adding a Foreign route reflector in a PE Network”
- “Adding a router in a route reflector PE Network”

Adding a PE network to the Administration Database

Add a new PE network that will support 2547 VPNs.

Prerequisites

You need the following values for the new PE network parameters:

- PE network name
- AS number for the new network
- Topology type

Procedure steps

1. In the tree hierarchy of the Service Provisioning - IP VPN Provider Edge window, right click on **All PE Networks**.
2. From the popup menu, select **Add new PE Network** to open the 2547 PE Network details panel.
3. In the **PE Network** field enter the PE network name.
4. In the **AS Number** field, enter the AS numbered assigned to the new PE network.
5. In the **Topology** list, select either Fully Peered Mesh or Route Reflector.
6. Optionally, in the **Description** field, type a description of the PE network.
7. Click **Apply** to add the PE network to the Administration Database.

Adding a router in a fully peered mesh PE Network

Add a Passport node as a router in the fully peered PE network and to the Administration Database.

Prerequisites

You need the following information:

- the name of the node to be used as a router for this PE network
- has the router object been provisioned on the node?

Procedure steps

1 In the tree hierarchy of the Service Provisioning - IP VPN Provider Edge window, right click on the 2547 PE network name.

2 From the popup menu, select **Add Router** to open the **Fully Peered Mesh Router** details panel.

3 In the **Node Type** field select **Passport**.

4 In the **Node Name** list, select the name of the node to be used as a PE Router.

5 If the router object has not yet been provisioned, go to step 6. Otherwise, go to step 7.

6 Click on the **Create Router Component...** button to launch a Nodal Provisioning session and provision the router component on the node. Then continue to step 7.

7 Optionally, in the **Description** field, type a description of the router.

8 Click **Apply**.

The **Router Name** field autofills with the node name and the Router instance. The primary loopback address is retrieved from the node and displayed in the **Primary Loopback Address** field.

The router is added to the Administration Database and associated with the selected PE network.

If this is the first router you add to the PE network, the procedure is completed. This router will be provisioned automatically when you use this procedure to configure the second router and complete step 9.

If this is not the first router, the **Provisioning Options Dialog** opens. Continue to step 9.

9 Select the provisioning options for the view on the node.

If you activate the provisioning, the PEP tool will start a provisioning session on every Passport in the PE Network.

The new router is added as a peer to each node. Each node is added as a peer to the new router. If this is the second router you add to the PE network, the first is now provisioned automatically.

ATTENTION	The PEP tool does not provision the Foreign node.

ATTENTION	If you do not select Activate, changes are not activated on the node and the Administration Database is not updated.

If the on-node provisioning is successfully activated, the appropriate components and links are created in the Administration Database.

ATTENTION	You may see a warning back from the node after the Check Prov. You can choose to proceed or not at this point.

Adding a Foreign router in a fully peered mesh PE Network

Add a Foreign (non-Nortel Networks) node as a router in the fully peered PE network and to the Administration Database.

Prerequisites

You need the following information:

- a name to be entered to represent the Foreign node
- a name to be entered to represent the router
- the primary loopback address of the Foreign router

Procedure steps

1. In the tree hierarchy of the Service Provisioning - IP VPN Provider Edge window, right click on the 2547 PE network name.
2. From the popup menu, select **Add Router** to open the **Fully Peered Mesh Router** details panel.
3. In the **Node Type** field select **Foreign**.

   The **Node Name**, **Router Name**, and **Primary Loopback Address** fields become text boxes. The **Create Router Component...** button disappears.
4. In the **Node Name** field, enter the name used to represent the Foreign node in the Administration Database.
5. In the **Router Name** field, enter the name used to represent the router in the Administration Database.
6. In the **Primary Loopback Address** field, enter the primary loopback address of the Foreign node, using IP address format.
7. Optionally, in the **Description** field, type a description of the router.
8. Click **Apply**.

   The **Provisioning Options Dialog** opens.
9. Select the provisioning options for the view on the Passport node.

   If you activate the provisioning, the PEP tool will start a provisioning session on every non-Foreign node in the PE Network. The provisioning sessions add the new Foreign router as a peer to every Passport node.

ATTENTION	The PEP tool does not provision the Foreign node.

If the on-node provisioning is successfully activated, the router is added to the Administration Database and associated with the selected PE network.

ATTENTION

If you do not select Activate, changes are not activated on the node and the Administration Database is not updated.

ATTENTION

You may see a warning back from the node after the Check Prov. You can choose to proceed or not at this point.

Adding a Foreign route reflector in a PE Network

Add a Foreign (non-Nortel Networks) node as a route reflector in a PE network with a route reflector topology.

Prerequisites

You need the following information:

- a name to be entered to represent the Foreign node
- a name to be entered to represent the router
- the primary loopback address of the Foreign router

Procedure steps

1 In the tree hierarchy of the Service Provisioning - IP VPN Provider Edge window, right click on the 2547 PE network name.

2 From the popup menu, select **Add Route Reflector** to open the **Route Reflector** details panel.

The Node Type field is read-only and is always set to **Foreign**.

The **Node Name**, **Router Name**, and **Primary Loopback Address** fields are text boxes.

3 In the **Node Name** field, enter the name used to represent the Foreign node in the Administration Database.

4 In the **Router Name** field, enter the name used to represent the router in the Administration Database.

5 In the **Primary Loopback Address** field, enter the primary loopback address of the Foreign node.

6 Optionally, in the **Description** field, type a description of the router.

7 Click **Apply**.

The route reflector is added to the Administration Database and associated with the selected PE network.

Adding a router in a route reflector PE Network

Add a Passport node as a router in a PE network with a route reflector topology.

Prerequisites

- At least one route reflector provisioned in the PE network.
- You need to know the following information:
  - the name of the node to be provisioned as a router for this PE network
  - has the router object been provisioned on the node?

Procedure steps

1 In the tree hierarchy of the Service Provisioning - IP VPN Provider Edge window, right click on the 2547 PE network name.

2 From the popup menu, select **Add Router** to open the **Router in a Reflector Network** details panel.

The Node Type field is read-only and is always set to **Passport**.

3 In the **Node Name** list, select the name of the node to be used as a PE Router.

4 If the router object has not yet been provisioned, go to step 5. Otherwise, go to step 6.

5 Click on the **Create Router Component...** button to launch a Nodal Provisioning session and provision the router component on the node. Then continue to step 6.

6 Optionally, in the **Description** field, type a description of the router.

7 In the **Route Reflector** list at the bottom of the details panel, click the appropriate check box to select the route reflector(s) to be peered with the new router.

8 Click **Apply**.

The **Provisioning Options Dialog** opens.

9 Select the provisioning options for the view on the node.

If you activate the provisioning, The PEP tool will start a provisioning session on the selected node. The provisioning session adds each route reflector you selected in step 7 as a peer to the new router.

ATTENTION The PEP tool does not provision the route reflector because it is always a Foreign node.

If the on-node provisioning is successfully activated, the router is added to the Administration Database and associated with the selected PE network.

ATTENTION If you do not select Activate, changes are not activated on the node and the Administration Database is not updated.

ATTENTION You may see a warning back from the node after the Check Prov. You can choose to proceed or not at this point.

Chapter 2
2547 IP VPN configuration

Use the IP VPN service provisioning (IP VPN SP) tool to configure an RFC 2547 VPN.

If you have used other methods to configure the 2547 VPNs in your PE network, you can discover them and then use the IP VPN SP tool to administer them.

For information about the discovery process and how to set up the PE network before you use the IP VPN SP tool to administer existing 2547 VPNs, see 241-6001-400 *Preside MDM Administration Database User Guide*

This document contains the following sections:

- "Prerequisites to 2547 VPN configuration" (page 27)
- "2547 VPN configuration procedures" (page 28)

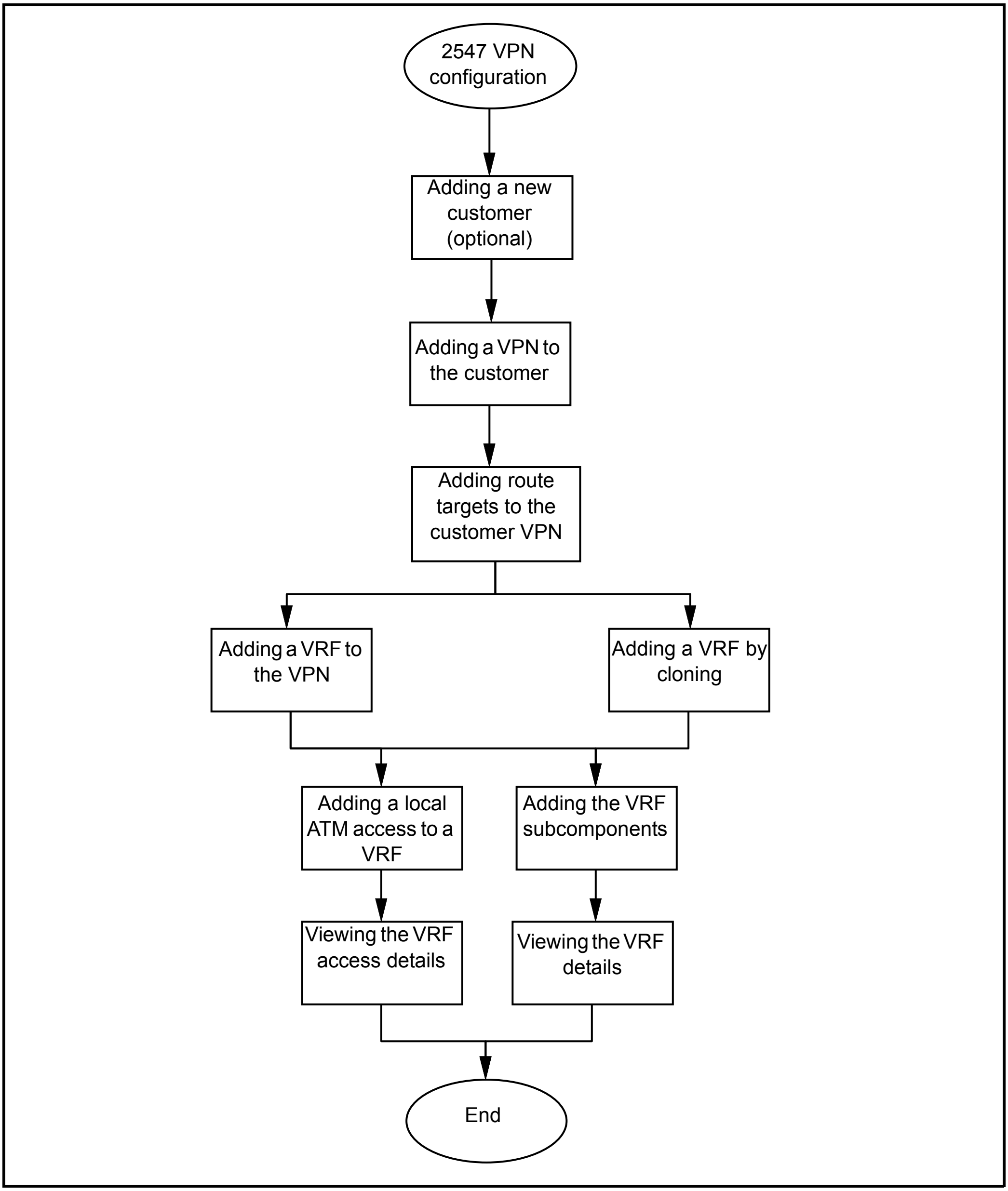
Prerequisites to 2547 VPN configuration

- Install and configure the Preside Multiservice Data Manager Administration Database to support VPNs. See 241-6001-400 *Preside MDM Administration Database User Guide*.
- Ensure that the PE network has been set up for 2547 VPNs. See "BGP peering configuration" (page 15).

2547 VPN configuration procedures

The task flow shows you the sequence of procedures you perform to configure a 2547 VPN. To link to any procedure in this document, double-click on the procedure name in the task flow or in the “2547 VPN configuration procedure navigation” (page 30) list.

Figure 2
2547 VPN configuration procedures


2547 VPN configuration
Adding a new customer (optional)
Adding a VPN to the customer
Adding route targets to the customer VPN
Adding a VRF to the VPN
Adding a VRF by cloning
Adding a local ATM access to a VRF
Adding the VRF subcomponents
Viewing the VRF access details
Viewing the VRF details
End

2547 VPN configuration procedure navigation

Adding a new customer (optional)

If the customer object does not exist in the Administration Database, you can add a new customer using the IP VPN SP tool.

ATTENTION	The customer in this procedure is an actual customer (not the Default Customer or the Service Provider Customer).

If you want to add administrative information about the customer, see 241-6001-400 *Preside MDM Administration Database User Guide*.

Procedure steps

1. In the tree hierarchy of the Service Provisioning - IP VPN window, right click on **All Customers**.
2. From the popup menu, select **Add new customer** to open the **Customer details** panel.
3. In the **Customer name** field enter the customer name.
4. Optionally, in the **Description** field, type a description of the customer.
5. Click **Apply** to add the customer to the Administration Database.

Procedure job aid

The following job aid provides information about possible error conditions.

Table 1
Possible error conditions when adding the customer object

Error condition	Corrective action
Customer name already exists.	Change the Customer Name.
Invalid customer name.	Review the reason for the error, as described in the dialog box, and correct the invalid Customer Name.
Error while the operation is in progress.	Review the reason for the error, as described in the dialog box, and correct it.

Adding a VPN to the customer

Add a new 2547 VPN to the customer using the IP VPN SP tool to create the logical entity in the Administration Database. This associates the VPN with the appropriate customer and PE network object.

Prerequisites

You need the following information:

- PE network name to which the VPN belongs
- name of the VPN to be added
- VPN maximum access points
- route targets to be assigned to the VPN

Procedure steps

1. In the tree hierarchy, select the Customer that you want to create a VPN for and right-click on the customer.

2. From the popup menu, select **Add new 2547 VPN**, to add a new VPN under the Customer in the tree.

   The VPN Details panel is displayed on the right side of the window.

3. In the **VPN Name** field, type the name for the VPN.

4. The **VPN Type** field is not editable. It specifies that this is a 2547 VPN.

5. In the **Max. Access Points** field, type the maximum number of access points for the VPN.

6. From the **PE Network Name** list, select a PE network from the list of existing PE Networks.

   If no PE network exists, you will get an error message when you apply the provisioning. See “Possible error conditions when adding a VPN” (page 33).

7. Add new Route Targets to the table of **Assigned Route Targets**. See “Adding route targets to the customer VPN” (page 34).

8. Optionally, type a free form description for the VPN in the **Description** field.

9. Click **Apply** to add the VPN to the customer in the Administration Database.

Procedure job aid

The following job aid provides information about possible error conditions.

Table 2
Possible error conditions when adding a VPN

Error	Corrective action
PE network name not defined in Administration Database	1. Create the PE network object in either of two ways: • using the IP VPN Provider Edge Provisioning tool. See “BGP peering configuration” (page 15). • using the Administration Database. See 241-6001-400 *Preside MDM Administration Database User Guide*. 2. Return to IP VPN SP tool and perform a refresh on the customer name to load the PE network into the tool. See “Refreshing customers and VPNs from the Administration Database” (page 71).
VPN name already exists.	Change the VPN Name.
Invalid VPN name	Review the reason for the error, as described in the dialog box, and correct the invalid VPN Name.
Error while the operation is in progress	Review the reason for the error, as described in the dialog box, and correct it.

Adding route targets to the customer VPN

Add the route targets (RT) to the customer VPN to control the communication rules between the customer sites in the VPN.

Prerequisites

- Understand the affect of changes to RTs on VPN discovery. See 241-6001-400 *Preside MDM Administration Database User Guide*, VPN Management.
- Understand “Route target rules” (page 35), “Special scenarios” (page 35), and “Possible warnings when adding route targets” (page 36).

Procedure steps

1. Select a VPN in the tree hierarchy.
2. To the right of the **Assigned Route Targets** section, click **Add...** to open the **Manage Route Targets** dialog box.
3. Add an RT in one of the following ways:
   - in the **Route Target** field manually enter a new RT.
   - click **Generate RT** to automatically generate an RT.
   - click **Browse...** to open the **All Route Targets** dialog box. Select an RT from the list and click **OK** to add the selected RT and return to the **Manage Route Targets** dialog.
4. If you have entered the RT manually, or generated the RT, select a customer for the RT from the **RT Owner** list.
5. Optionally, in the **Description** field, add information about the RT.
6. Click **OK** to add the RT and return to the VPN Details panel.

Procedure job aid

The following job aid provides information about:

- “Route target rules” (page 35)
- “Special scenarios” (page 35)
- “Possible warnings when adding route targets” (page 36)

Table 3
Route target rules

Rule #	Route target rule
1	For a VPN customer, an RT is an intranet RT in a VPN when both the RT and the VPN are owned by that customer.
2	A VPN being created must have at least one intranet RT.
3	For a VPN customer, an RT owned by that customer that is added to another VPN owned by the same customer causes the two VPNs to merge into one VPN.
4	For a VPN customer, an RT is marked as an extranet RT in a VPN if EITHER of the following is true: • the VPN customer does not own the RT • the RT owned by the VPN customer is included in another VPN that is owned by another customer
5	Customer-owned RTs must not be included in any Service Provider VPN.

Table 4
Special scenarios

Scenario	Result
Existing 2547 VPNs have not been configured using the IP VPN SP tool.	Discovery assigns existing RTs to the Default Customer object in the Administration Database. Once you create the customer objects in the Administration Database you must reassign the RTs to the appropriate customers.
(Sheet 1 of 2)	

Table 4
Special scenarios

Scenario	Result
Customer A owns an RT that is included in VPN A1. Customer A changes the owner of the RT to Customer B.	Discovery is automatically initiated and the following occurs: • VPN A1 retains the RT as an extranet RT • if Customer B does not have a VPN that is already using this RT, a new VPN s created for Customer B with the RT included in that new VPN.
Customer A creates a new RT for VPN A1 and sets the owner as Customer B.	Discovery is automatically initiated and the following occurs: • the new RT is added to VPN A1 as an extranet RT. • a new VPN is created for Customer B that includes the new RT.
(Sheet 2 of 2)	

Table 5
Possible warnings when adding route targets

Warning	Action
Warning that another VPN already uses this RT and that the two VPNs will be merged.	You are attempting to merge two VPNs. If this is what you want to do, you can proceed. Otherwise, correct the RT or cancel the procedure.
Warning that by adding an RT owned by a customer other than the current one could give external access to VPNs that include this RT.	You are attempting to add an extranet route target. If this is what you want to do, you can proceed. Otherwise, correct the RT or cancel the procedure.

Adding a VRF to the VPN

Add a virtual router function (VRF) to the customer VPN using the IP VPN SP tool. This associates the Route Distinguisher (RD) and Route Targets (RT) to the VRF at the VPN site.

ATTENTION	Optionally, you can clone an existing VRF to add subsequent VRFs to the VPN. See “Adding a VRF by cloning” (page 41).

Prerequisites

You need the following information for each VRF:

- node name and name of the VRF to be added
- if you are not planning to use the auto-generate process, the RD associated with the VRF that is unique throughout the PE network
- RTs to be added to the VRF
- applicable import/export mode for each Route Target assigned to the VRF

Procedure steps

1 In the hierarchy tree in the IP VPN Service Provisioning window, right click on the 2547 VPN to which you wish to add a VRF.

2 From the popup menu, select **Manage VRFs...**.

The **VPN Routing Function Management** dialog box opens.

3 Click **New** to add a new VRF to the VPN.

The fields in the **VRF Routing Details** clear.

4 In the **Node** panel, select a node from the **Node Name** list.

5 Deselect **Use Defaults** if you wish to override the default user ID and password, and type a user ID and password in the **User ID** and **Password** fields.

6 In the **VRF** panel, you can do either of the following:

- type a VRF instance name in the **VRF Name** field and go to step 7.
- add an existing VRF. See “Adding an existing VRF” (page 40) then return to step 8 of this procedure.

7. In the **Route Distinguisher** field, enter the appropriate RD or click **Generate RD** to auto generate a new RD.

8. Optionally in the Description field, enter information about the role of the VRF in the VPN topology.

9. In the Route Targets panel, from the list of **Available RTs in this VPN**, select an RT.

10. Click **Add RT to VRF**.

    The RT displays in the list of **Selected RTs in current VRF**.

11. Optionally, review the list of VRFs that will be exchanging routes as a result of adding the route target in step 10. With the RT still selected, click **Show VRFs Common to RT...**.

    The **Common VRFs for Route Target** dialog opens.

12. Click **OK** to return to the **VRF Management** dialog.

13. Click **Apply**.

    The **Provisioning Options Dialog** opens.

14. Select the provisioning options for the view on the node.

ATTENTION	If you do not select Activate, changes are not activated on the node and the Administration Database is not updated.

If the on-node provisioning is successfully activated, the appropriate components and links are created in the Administration Database. See “Possible error conditions when adding a VRF to the VPN” (page 39).

ATTENTION	You may see a warning back from the node after the Check Prov. You can choose to proceed or not at this point.

15. Optionally, review all the VRF details. See “Viewing the VRF details” (page 76).

Procedure job aid

The following job aid provides information about possible error conditions.

Table 6
Possible error conditions when adding a VRF to the VPN

Error condition	Action
You have entered an RD in the **Route Distinguishe**r field. Check Prov fails and you see a warning that the RD must be unique.	Correct the RD and click Apply again. NOTE: If you have used Generate RD, the RD will be unique in the Administration Database.
Warning that prerequisite data is missing.	Click OK to acknowledge the missing data. The IP VPN SP tool automatically cancels the procedure.
If any of the data is invalid, a message dialog box opens indicating which field is invalid and why.	Correct the invalid data and click Apply again.
If an error occurs while the operation is in progress, a message dialog box shows the error, the operation stops, and the tool disconnects from the node.	Review the data you have entered and correct if necessary. Click Apply again. The node could be temporarily busy and not responding.

Adding an existing VRF

Add an existing VRF to the customer VPN by browsing through all VRFs common to the PE Router for the specified node.

Prerequisites

- at least one VRF exists under the PE Router on the specified node.
- you are in the process of "Adding a VRF to the VPN" (page 37).

Procedure steps

1 Click the **....** to the right of the **VRF** Name field.

The **Common VRFs for Node** dialog box opens.

2 Select a VRF from the list.

3 Click **OK** to return to the **VRF Management** dialog.

The VRF fields are populated automatically except for the **Description**.

Procedure job aid

The following job aid provides information about possible error conditions:

Table 7
Possible error conditions when adding an existing VRF

Error condition	Corrective action
Warning that VRF has existing RTs that are not part of the VPN list of RTs.	To include this VRF, close the VRF Management dialog and add the RTs to the VPN. See "Adding route targets to the customer VPN" (page 34). Then return to the procedure "Adding an existing VRF" (page 40).

Adding a VRF by cloning

Add a VRF to the customer VPN by cloning an existing VRF to reduce the amount of information you need to enter in the VPN Routing Function Details panel.

Prerequisites

You need the following information:

- at least one VRF exists in the customer VPN.
- **Clone VRF on Creation** enabled from the Options menu in the Service Provisioning - IP VPN window. See "Options" (page 87) for information about this option.
- Node name and name of the VRF to be added
- RD associated with the VRF that is unique throughout the PE network
- If applicable, RTs to be added to the VRF

Procedure steps

1 In the tree hierarchy of the Service Provisioning - IP VPN window, right click on the VPN name.

2 From the popup menu, select **Manage VRFs...**.

The **VRF Management** dialog opens.The table at the top of the dialog displays a list of VRFs that you have already added to the selected VPN.

3 From the VRF list, select the VRF you want to clone.

The VPN Routing Function Details are displayed.

4 Click the **New** button at the bottom of the panel.

If you see a Clone VRF confirmation dialog go to step 5.

If you do not see a Clone VRF confirmation dialog, go to step 8.

5 Click **Yes**.

6 Optionally, select **Don't ask again** to prevent this dialog from appearing each time you click **New**.

This will automate VRF cloning without the confirmation dialog each time you click on the **New** button to add a new VRF.

7 Click **OK**.

The **PE Network Name**, **VRF Name**, list of **Available RTs in this VPN** and list of **Selected RTs in current VRF** remain unchanged.The **Node Name**, **PE Router**, and **Description** fields are cleared.

8 From the **Node Name** list, select a new node name.

The **PE Router** field is automatically filled.

9 Optionally, enter a new VRF name in the **VRF Name** field.

10 In the **Route Distinguisher** field, enter the appropriate RD or click **Generate RD** to auto generate a new RD.

11 Optionally, add more RTs to the list or remove RTs from the list.

12 Click **Apply**.

The **Provisioning Options Dialog** opens.

13 Select the provisioning options for the view on node.

ATTENTION	If you do not select Activate, changes are not activated on the node and the Administration Database is not updated.

If the on-node provisioning is successfully activated, the appropriate components and links are created in the Administration Database.

ATTENTION	You may see a warning back from the node after the Check Prov. You can choose to proceed or not at this point.

14 Optionally, review all the VRF details. See “Viewing the VRF details” (page 76).

Adding the VRF subcomponents

Add the subcomponents to the VRF.

Prerequisites

- VRF added to the customer VPN in the Administration Database and provisioned on the PE node.

Procedure steps

1 In the tree hierarchy of the Service Provisioning - IP VPN window, right click on the VPN name.

2 From the popup menu, select **Manage VRFs...**.

The **VRF Management** dialog opens.The table at the top of the dialog displays a list of VRFs that you have already added to the selected VPN.

3 From the VRF list, select the VRF you want to view.

The VRF details are populated to the VRF Summary section.

4 Select the **VRF Details** tab.

5 In the **Component to modify** picklist, select the component (OSPF, BGP, RIP Ext Policy, Diffserv, General VRF, or CAS) that you want as the starting point for the IP VPN SP tool to load.

The component tree hierarchy loads in the left panel of the VRF Details.

6 Right-click on the component or attribute to open the popup menu and select **add subcomponent...**.

The **Subcomponent Selection** dialog opens.

7 In the Subcomponent Selection picklist, select the component that you want to add.

8 Click OK.

The dialog closes and the component is added to the component tree hierarchy.

9 Click **Apply**.

The **Provisioning Options Dialog** opens.

10 Select the provisioning options for the view on the node.

ATTENTION	If you do not select Activate, changes are not activated on the node and the Administration Database is not updated.

If the on-node provisioning is successfully activated, the appropriate components and links are created in the Administration Database.

ATTENTION	You may see a warning back from the node after the Check Prov. You can choose to proceed or not at this point.

11 Optionally, review all the VRF access details. See “Viewing the VRF access details” (page 75).

Adding a local ATM access to a VRF

Add a local ATM access to a VRF to provide customer site access to the VPN.

Prerequisites

- physical ports are provisioned
- VRFs are assigned to the VPN

Procedure steps

1 In the tree hierarchy of the Service Provisioning - IP VPN window, right click on the VPN name.

2 From the popup menu, select **Manage VRFs...**.

The **VRF Management** dialog opens.The table at the top of the dialog displays a list of VRFs that you have already added to the selected VPN.

3 From the VRF list, select the VRF you want to associate with the local ATM access.

4 Select the **VRF Access** tab.

5 From the **Access Type** picklist, select Local ATM.

6 In the **Site** field, enter the site name or click **...** to browse for an existing name.

7 From the **Port** picklist, select a port interface to associate with the Local ATM access method. If the selected port is currently unassigned, go to step 8. If the selected port is already assigned to an AtmIf, the AtmIf field is automatically populated with the associated ATM interface instance. Go to step 9.

8 In the **AtmIf** field, enter the AtmIf instance.

9 In the **VCC** table, enter the vpi and vci for each class of service.

10 Optionally, in the **Access Point** field, enter a name for the Local ATM access. Otherwise, click on the **Use IP Logical Interface** checkbox to use the IP logical interface as the name for the access point.

The **Access Point** field displays the IP logical interface name as a read-only entry.

11 In the **Logical Interface** field, enter the IP address and network mask in the format <IP address>/<network mask>.

12 Click **Apply**.

The **Provisioning Options Dialog** opens.

13 Select the provisioning options for the view on the node.

ATTENTION If you do not select Activate, changes are not activated on the node and the Administration Database is not updated.

If the on-node provisioning is successfully activated, the appropriate components and links are created in the Administration Database. See “Possible error conditions when adding a VRF to the VPN” (page 39).

ATTENTION You may see a warning back from the node after the Check Prov. You can choose to proceed or not at this point.

Configuring additional components of the VRF access

Configure additional components of the VRF access media.

Prerequisites

- physical ports are provisioned
- VRFs are assigned to the VPN
- VRF access media provisioned on the node

Procedure steps

1. In the tree hierarchy of the Service Provisioning - IP VPN window, select and expand the customer object.
2. Right-click on the appropriate VPN name.
3. From the popup menu, select **Manage VRFs...**.

   The **VRF Management** dialog opens.The table at the top of the dialog displays a list of VRs that you have already added to the selected VPN.
4. From the VRF list, select the VRF you want to view.

   The VRF details are populated to the VRF Summary section.
5. Select the **VRF Access** tab.
6. In the bottom panel of the window, select the **Access Detail**s tab.
7. In the **Component to modify** picklist, select the component (Port, Media, Logical Interface, or Service Interface) that you want as the starting point for the IP VPN SP tool to load.

   The component tree hierarchy loads in the left panel of the Access Details.
8. Optionally, right-click on the component or attribute to open the popup menu and select **Add sub-component..., Modify...** or **Delete**.

   A dialog box opens showing the attributes of the component/sub-component that you have selected.
9. Complete the appropriate entries in the dialog box and click **OK**.
10. Click **Apply**.

    The **Provisioning Options Dialog** opens.
11. Select the provisioning options for the view on the node.

ATTENTION If you do not select Activate, changes are not activated on the node and the Administration Database is not updated.

If the on-node provisioning is successfully activated, the appropriate components and links are created in the Administration Database.

ATTENTION You may see a warning back from the node after the Check Prov. You can choose to proceed or not at this point.

Chapter 3
2764 autodiscovered VPN configuration

Use the IP VPN service provisioning (IP VPN SP) tool to configure an RFC 2764 VPN with autodiscovery enabled.

If you have used other methods to configure the 2764 VPNs with autodiscovery enabled in your PE network, you can discover them and then use the IP VPN SP tool to administer them.

For information about the discovery process and how to set up the PE network before you use the IP VPN SP tool, see 241-6001-400 *Preside MDM Administration Database User Guide*

ATTENTION	You cannot use the IP VPN Service Provisioning tool to configure and manage VPNs on Passport 6000 nodes loaded with P7.0.x software.

This document contains the following sections:

- "Prerequisites to 2764 autodiscovered VPN configuration" (page 49)
- "2764 autodiscovered VPN configuration procedures" (page 50)

Prerequisites to 2764 autodiscovered VPN configuration

- Configure the VCG backbone between the provider edge (PE) nodes. See NN10600-582 *Passport 7400, 15000, 20000 VPN Configuration Management* for the following procedures:
  - — *Configuring management VR and VCG on the node*
  - — *Configuring an inter-VR virtual media link*

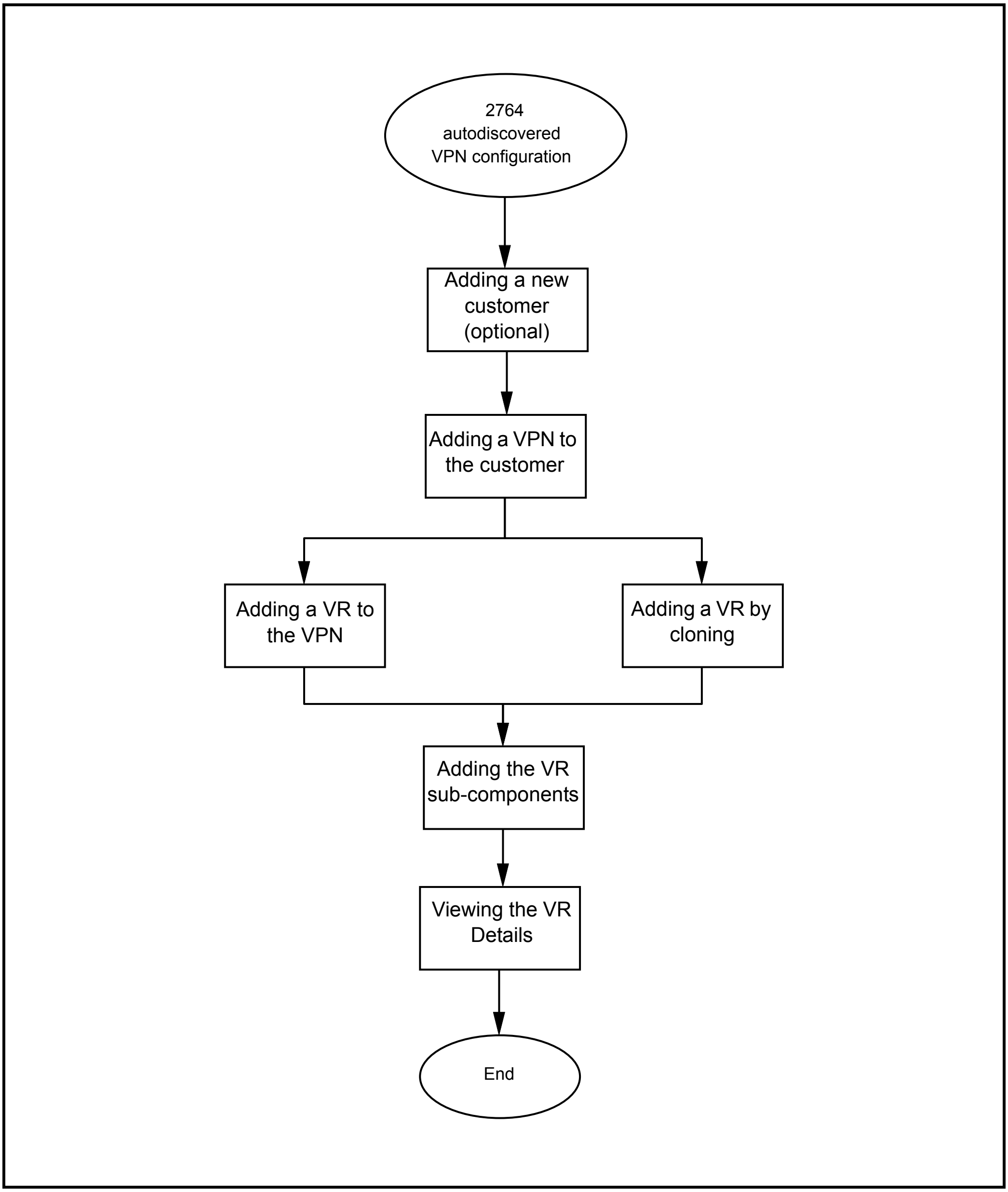
— *Configuring backbone connections between VCGs over ATM (PVCs or soft PVCs)*

- Install and configure the Preside Multiservice Data Manager Administration Database to support VPNs. See 241-6001-400 *Preside MDM Administration Database User Guide*.
- For each Passport PE node, ensure that the views containing the VCG definitions have been loaded into the Administration Database through the database synchronization process. The VCGs are represented in the Administration Database as PE router objects
- In the Administration Database, create the PE network object and assign each PE router object to the PE network. See 241-6001-400 *Preside MDM Administration Database User Guide*.

2764 autodiscovered VPN configuration procedures

The task flow shows you the sequence of procedures you perform to configure an 2764 autodiscovered VPN. To link to any procedure in this document, double-click on the procedure name in the task flow or in the "2764 autodiscovered VPN configuration procedures navigation" (page 52) list.

Figure 3
2764 VPN configuration procedures


2764 autodiscovered VPN configuration
Adding a new customer (optional)
Adding a VPN to the customer
Adding a VR to the VPN
Adding a VR by cloning
Adding the VR sub-components
Viewing the VR Details
End

2764 autodiscovered VPN configuration procedures navigation

Adding a new customer (optional)

If the customer object does not exist in the Administration Database, you can add a new customer using the IP VPN SP tool.

ATTENTION	The customer in this procedure is an actual customer (not the Default Customer or the Service Provider Customer).

If you want to add administrative information about the customer, see 241-6001-400 *Preside MDM Administration Database User Guide*.

Procedure steps

1. In the tree hierarchy of the Service Provisioning - IP VPN window, right click on **All Customers**.
2. From the popup menu, select **Add new customer** to open the **Customer details** panel.
3. In the **Customer name** field enter the customer name.
4. Optionally, in the **Description** field, type a description of the customer.
5. Click **Apply** to add the customer to the Administration Database.

Procedure job aid

The following job aid provides information about possible error conditions.

Table 8
Possible error conditions when adding the customer object

Error condition	Corrective action
Customer name already exists.	Change the Customer Name.
Invalid customer name.	Review the reason for the error, as described in the dialog box, and correct the invalid Customer Name.
Error while the operation is in progress.	Review the reason for the error, as described in the dialog box, and correct it.

Adding a VPN to the customer

Add a new 2764 VPN to the customer using the IP VPN SP tool to create the logical entity in the Administration Database. This associates the VPN with the appropriate customer and PE network object.

Prerequisites

- you need the following information
  - VPN identifier number
  - ASN for BGP routing
  - private address space

Procedure steps

1. In the tree hierarchy of the Service Provisioning - IP VPN window, right click on the customer name.
2. From the popup menu, select **Add new 2764 VPN**.

   This adds the VPN to the tree hierarchy and selects it. The **VPN Details** panel is displayed on the right side of the window.
3. In the **VPN name** field, type the VPN name.
4. In the **VPN identifier** field, type a unique VPN identifier using the appropriate format.
5. If the VPN will not be MBGP enabled, then in the **AS ID** field, type the autonomous system number for BGP routing. If the VPN will be MBGP enabled, go to step 6
6. From the **PE Network Name** list, select the PE network to which the VPN belongs.
7. In the Private Network Address field, enter the IP address space.
8. If you selected an MBGP PE network in step 6, optionally click the Enable Multi-Protocol BGP check box to set the MBGP option on the VRs you add to the VPN. See “Adding a VR to the VPN” (page 55)
9. Optionally, type a free form description for the VPN in the **Description** field.
10. Click **Apply** to add the VPN to the customer in the Administration Database.

Adding a VR to the VPN

Add a virtual router (VR) to the customer VPN using the IP VPN SP tool. This creates the customer VR and the inter-VR tunnel between the customer VR and the VCG.

ATTENTION	Optionally, you can clone an existing VR to add subsequent VRs to the VPN. See “Adding a VR by cloning” (page 60).

Prerequisites

- you need the following on-node information for each PE
  - inter-VR tunnel interface address
  - optionally, the public IP aggregation addresses

Procedures

1. In the tree hierarchy of the Service Provisioning - IP VPN window, right click on the VPN name.
2. From the popup menu, select **Manage VRs...**.

   The **Virtual Router Management** dialog opens.The table at the top of the dialog displays PEs and VRs that you have added to the selected VPN. Otherwise it will be empty.
3. Select the **VR Summary** tab.
4. Click the **New** button at the bottom of the panel.
5. In the **Node** panel, **Node Name** field, select a PE node name from the list.

   The read-only fields in the **PE Network** panel display the PE Network Name and Virtual Carrier Gateway associated with the PE node.
6. Optionally deselect **Use Defaults** if you do not wish to use the default User ID and password. Enter a user ID and password.
7. Optionally in the **Virtual Router** panel, **Virtual Router Name** field, change the virtual router name. By default, the VPN is present.
8. In the **Inter-VR Tunnel** panel, add a Private Logical Interface IP and Mask.

9 Optionally, deselect **Enable Public IP Aggregation** to disable the Public Source End Point field and automatically populate it using the IP from the **Public Logical Interface** field.

The Public Logical Interface and the **Public Source Endpoint** are now identical. The Public Source Endpoint becomes read only.

10 If you have not enabled MBGP in the VPN panel, then in the **Routing** panel, **BGP** section, select either Route Reflector, or, select Hub or Spoke. Then go to step 12. If you have enabled MBGP, go to step 11.

If you select Route Reflector, the Hub radio button is automatically set. The Hub and Spoke buttons become read-only.

11 In the **Routing** panel, specify the **Multi-Protocol BGP** specific attributes:

- Specify an **MBGP Route Preference**.
- In the **Import Route Limit** field, specify the maximum number of MBGP routes that can be imported from VCG BGP Ribin.
- In the **Export Route Limit**, specify the maximum number of Customer VR routes that can be exported into a VCG BGP Ribin.

12 Optionally, in the **IP CoS Profiles** panel, select an Access IP CoS Profile and Core IP CoS Profile, or select None for each, if no IP CoS is required. Alternately, you can click the browse button [...] to the right of each field to open the IP CoS Profile Editor. See “Adding an IP CoS Profile” (page 58) to view, add, delete, and modify available profiles.

13 Click **Apply**.

The **Provisioning Options Dialog** opens.

14 Select the provisioning options for the view on the node.

ATTENTION	If you do not select Activate, changes are not activated on the node and the Administration Database is not updated.

If the on-node provisioning is successfully activated, the appropriate components and links are created in the Admin DB. See “Possible error conditions when adding a VR to the VPN” (page 57).

ATTENTION	You may see a warning from the node after the Check Prov. You can choose to proceed or not at this point.

15 Optionally, review all the VR details. See “Viewing the VR Details” (page 79).

Procedure job aid

The following job aid provides information about possible error conditions.

Table 9
Possible error conditions when adding a VR to the VPN

Error condition	Corrective action
Warning that prerequisite data is missing	Cancel the procedure and return to the appropriate tool and relevant procedure to enter the missing data.
If any of the data is invalid, a message dialog box opens indicating which field is invalid and why.	Correct the invalid data and click Apply again.
If an error occurs while the operation is in progress, a message dialog box shows the error, the operation stops, and the tool disconnects from the node.	Read the message. If it is about the data you have entered, correct the data and click Apply again. Otherwise, contact your technical administrator.

Adding an IP CoS Profile

You can add an IP CoS Profile. There are two types of Class of Service (CoS) profiles: Access and Core.

The Access IP CoS Profile is the default IP CoS for the access circuits connecting to the customer VR. The Core IP CoS Profile applies to the connection between the customer VR and the PE node VCG.

Prerequisites

- the IP VPN service provisioning tool is started

Procedure steps

1. Launch the IP CoS Editor from the VR Management dialog.

   The Edit/View 2764 IP Class of Service dialog box opens.

2. From the Profile Name list, select or type a name.
3. Type a description in the Description field.
4. In the ToS Marking panel, check the ToS Marking for CoS index, ToS Value, and ToS Mask fields.
5. Optionally, add one or more policies by clicking Add... next to CoS Policies list to open the Add New CoS Policy dialog box.
6. Complete the Policy, CoS Index and ToS Map fields
7. Optionally, add one or more Flow Classifications for a given policy by clicking Add... to the right of the Flow Classification list to open the Add New Cos Policy dialog box.
8. Enter a Flow Classification Identifier, select a Protocol, and complete the Port, Prefix and Prefix Length fields.
9. Click OK, to close the dialog box and return to the Add New CoS Policy dialog box.

   The flow classifications which you added are listed in the Flow Classification list.

10. Click OK to close the Add New CoS Policy dialog box.
11. In the Edit/View IP Class of Service dialog box, click Save to save the IP CoS Profile to the Administration Database.

    The version is incremented to the next available index with the same Profile Name.

If you have entered invalid values, and error message opens. Correct the errors and click Save again.

12 Click Close to close the IP CoS Editor.

The currently selected Profile will be selected in the list adjacent to the launch point.

Adding a VR by cloning

Add a VR to the customer VPN by cloning an existing VR to reduce the amount of information you need to enter in the VR Summary form.

Prerequisites

- at least one VR exists in the customer VPN.
- **Clone VR on Creation** enabled from the Options menu in the Service Provisioning - IP VPN window. See “Options” (page 87) for information about this option.

Procedure steps

1 In the tree hierarchy of the Service Provisioning - IP VPN window, right click on the VPN name.

2 From the popup menu, select **Manage VRs...**.

The **Virtual Router Management** dialog opens.The table at the top of the dialog displays a list of VRs that you have already added to the selected VPN.

3 From the VR list, select the VR you want to clone.

4 Select the **VR Summary** tab.

The VR details are displayed.

5 Click the **New** button at the bottom of the panel.

If you see a Clone VR confirmation dialog go to step 6.

If you do not see a Clone VR confirmation dialog, go to step 9.

6 Select Yes.

7 Optionally, select **Don’t ask again** to disable the confirmation dialog.

This will automate VR cloning without the confirmation dialog each time you click on the **New** button to add a new VR.

8 Click OK.

The Node Name field clears.

9 In the **Node** panel, **Node Name** field, select a new PE name from the list.

10 Optionally, change any other of the fields in the VR Summary details using the relevant steps from the procedure in “Adding a VR to the VPN” (page 55).

11 Click **Apply**.

The **Provisioning Options Dialog** opens.

12 Select the provisioning options for the view on the node.

ATTENTION	If you do not select Activate, changes are not activated on the node and the Administration Database is not updated.

If the on-node provisioning is successfully activated, the appropriate components and links are created in the Administration Database. See “Possible error conditions when adding a VR to the VPN” (page 57).

ATTENTION	You may see a warning back from the node after the Check Prov. You can choose to proceed or not at this point.

13 Optionally, review all the VR details. See “Viewing the VR Details” (page 79).

Adding the VR sub-components

Add the sub-components to the VR by launching the embedded nodal provisioning (ENP) tool.

Prerequisites

- VR added to the customer VPN in the Administration Database and provisioned on the PE node.

Procedure steps

1 In the tree hierarchy of the Service Provisioning - IP VPN window, right click on the VPN name.

2 From the popup menu, select **Manage VRs...**.

The **Virtual Router Management** dialog opens.The table at the top of the dialog displays a list of VRs that you have already added to the selected VPN.

3 From the VR list, select the VR you want to view and right-click to display the popup menu.

4 Select the component (OSPF, BGP, RIP, General VR, or CAS Root) that you want as the starting point for the IP VPN SP tool to load.

The result displays in the left section of the VR Details panel.

5 In the left section of the VR Details panel, right-click on the VR to display the popup menu.

6 Select **add subcomponent...**.

ENP is launched.

7 Add the new sub-components by responding to the **ENP** prompts.

8 Optionally, review all the VR details. See “Viewing the VR Details” (page 79).

Chapter 4 Administering VPNs

Administer your customer VPNs using the IP VPN Provider Edge Provisioning (PEP) tool and the IP VPN Service Provisioning (SP) tool.

Navigation

Use the IP VPN PEP tool to perform the following administration procedures on the 2547 VPNs:

- “Changing the peers of a router in a route reflector PE network” (page 65)
- “Deleting a PE Router from a fully peered PE Network” (page 66)
- “Deleting a PE router from a route reflector PE Network” (page 67)

Use the IP VPN SP tool to perform the following administration procedures on the 2547 VPNs:

- “Deleting a customer” (page 68)
- “Modifying a Customer” (page 69)
- “Deleting a VPN” (page 70)
- “Refreshing customers and VPNs from the Administration Database” (page 71)
- “Deleting a VRF from an existing 2547 VPN” (page 72)
- “Modifying a 2547 VPN” (page 74)
- “Viewing the VRF access details” (page 75)
- “Viewing the VRF details” (page 76)

- “Removing a route target from a 2547 VPN” (page 77)

Use the IP VPN SP tool to perform the following administration procedures on the 2764 VPNs with auto-discovery enabled:

- “Deleting a customer” (page 68)
- “Modifying a Customer” (page 69)
- “Deleting a VPN” (page 70)
- “Refreshing customers and VPNs from the Administration Database” (page 71)
- “Modifying a 2764 VPN” (page 78)
- “Viewing the VR Details” (page 79)
- “Deleting a VR from an existing 2764 VPN” (page 80)
- “Deleting an IP CoS Profile from a VR” (page 81)

Changing the peers of a router in a route reflector PE network

Use the IP VPN PEP tool to change the peers of a router provisioned in a route reflector PE network.

Prerequisites

- IP VPN Provider Edge Provisioning tool main window is open.

Procedure steps

1 Select the router from the tree hierarchy of the Service Provisioning - IP VPN Provider Edge main window.

The **Router in a Route Reflector Network** details display the information about the selected router.

2 In the **Route Reflector** list at the bottom of the details panel, click on the box beside the appropriate the route reflector name to check (add) or uncheck (remove) the route reflector.

3 Click **Apply**.

The **Provisioning Options Dialog** opens.

4 Select the provisioning options for the view on the node.

If you activate the provisioning, the PEP tool will start a provisioning session on the selected Passport node.

ATTENTION	The PEP tool does not provision the route reflector to change its peering information because it is a Foreign node.

If the on-node provisioning is successful, the route reflectors are added or deleted as peers of the selected router.

ATTENTION	If you do not select Activate, changes are not activated on the node and the Administration Database is not updated.

ATTENTION	You may see a warning back from the node after the Check Prov. You can choose to proceed or not at this point.

Deleting a PE Router from a fully peered PE Network

Use the IP VPN PEP tool to delete a router from a PE network with a fully peered mesh topology.

Prerequisites

- IP VPN Provider Edge Provisioning tool main window is open.

Procedure steps

1 Select the router in the tree hierarchy of the Service Provisioning - IP VPN Provider Edge main window.

The **Fully Peered Mesh** Router details display the information about the selected router.

2 Right-click on the router and select Delete Peering...from the popup menu.

A confirmation dialog opens.

3 Click **Yes** to continue with the procedure.

4 Click **Apply**.

The **Provisioning Options Dialog** opens.

5 Select the provisioning options for the view on the node.

If you activate the provisioning, the PEP tool will start a provisioning session on every Passport in the PE network.

ATTENTION	The PEP tool does not provision the route reflector to remove its peering information because it is a Foreign node.

If the on-node provisioning is successful, the peer reference for the selected router is removed from each node. All peer references are removed from the selected router.

The router is disassociated from the PE Network in the Administration Database.

ATTENTION	If you do not select Activate, changes are not activated on the node and the Administration Database is not updated.

ATTENTION	You may see a warning back from the node after the Check Prov. You can choose to proceed or not at this point.

Deleting a PE router from a route reflector PE Network

Use the IP VPN PEP tool delete a router from a PE network with a route reflector topology.

Prerequisites

- IP VPN Provider Edge Provisioning tool main window is open.

Procedure steps

1 Select the router in the tree hierarchy of the Service Provisioning - IP VPN Provider Edge main window.

The **Route Reflector** details display the information about the selected router.

2 Right-click on the router and select Delete Peering...from the popup menu.

A confirmation dialog opens.

3 Click **Yes** to continue with the procedure.

4 Click **Apply**.

The **Provisioning Options Dialog** opens.

5 Select the provisioning options for the view on the node.

If you activate the provisioning, the PEP tool will start a provisioning session on the selected router.

ATTENTION	The PEP tool does not provision the route reflector to remove its peering information because it is a Foreign node.

If the on-node provisioning is successful, all peer references are removed from the selected router.

The router is disassociated from the PE Network in the Administration Database.

ATTENTION	If you do not select Activate, changes are not activated on the node and the Administration Database is not updated.

ATTENTION	You may see a warning back from the node after the Check Prov. You can choose to proceed or not at this point.

Deleting a customer

Use the IP VPN SP tool to delete a customer object from the Administration Database.

Prerequisites

- no references to the customer in the Administration Database
- IP VPN Service Provisioning tool main window is open

Procedure steps

1 Select a Customer in the tree hierarchy in the Service Provisioning - IP VPN main window.

2 Right click on the Customer and click **Delete**.

A dialog box displays asking you to confirm the delete action.

3 Click **Yes**.

If the customer has no references to it in the Administration Database, the customer is removed from the tree hierarchy and the All Customers item is selected.

If the customer has references to it in the Administration Database, the delete process is stopped.

Modifying a Customer

Use the IP VPN SP tool to modify a Customer object and update it in the Administration Database.

Prerequisites

- the Customer that you are modifying is stored in the database
- IP VPN Service Provisioning tool main window is open

Procedure steps

1 Select a Customer in the tree hierarchy in the Service Provisioning - IP VPN main window.

The **Apply** and **Cancel** command buttons are disabled.

2 Make your desired changes to the description in the Customer Details panel.

The **Apply** and **Cancel** buttons become enabled.

3 Click **Apply**.

The status changes to **Stored in the Administration Database**.

Deleting a VPN

Use the IP VPN SP tool to delete a 2547/2764 VPN object from the Administration Database.

Prerequisites

- all VRs/VRFs removed from the VPN
- IP VPN Service Provisioning tool main window is open

Procedure steps

1 Select a VPN under a customer in the tree hierarchy in the Service Provisioning - IP VPN main window.

2 Right click on the VPN and click **Delete**.

A dialog box displays asking you to confirm the delete action.

3 Click **Yes**.

If the VPN has no other VRs/VRFs associated with it in the Administration Database, the VPN is removed from the tree hierarchy and the customer item is selected.

If the VPN has at least one remaining VR/VRF associated with it in the Administration Database, the delete process is stopped.

Procedure job aid

The following job aid provides information about possible error conditions when deleting a 2547 VPN:

Table 10
Possible error conditions when deleting a 2547 VPN

Error condition	Corrective action
Warning to indicate that the route target is currently being used by VRFs in the VPN and cannot be deleted.	Remove the route target from each of the VRFs that use it. Otherwise, you can cancel the procedure and just remove selected route targets.

Refreshing customers and VPNs from the Administration Database

Refresh the IP VPN SP tool tree hierarchy customers and VPNs from the Administration Database.

ATTENTION	For 2547 VPNs, the VPNs are refreshed each time you change the RT ownership. This is because a change in the RT ownership could merge or split the existing 2547 VPNs

Prerequisites

- IP VPN Service Provisioning tool main window is open

Procedure steps

1. Select the **All Customers** item in the tree hierarchy of the Service Provisioning - IP VPN main window.
2. Right-click and from the pop-up menu, select **Refresh** to refresh the customers in the tree hierarchy.
3. Select a customer item in the tree hierarchy of the Service Provisioning - IP VPN main window.
4. Right-click and from the pop-up menu, select **Refresh** to refresh the customer’s VPNs in the tree hierarchy.

ATTENTION	An implicit refresh is performed by the IP VPN SP tool the first time a Customer item is expanded in the tree hierarchy. You can enable the **Force VPN reload on customer expansion option** so that the VPN data refreshes on subsequent expansions of the customer item. See “Options” (page 87).

Deleting a VRF from an existing 2547 VPN

Use the IP VPN SP tool to delete a VRF from an existing 2547 VPN. You must delete all VRFs before you can delete the VPN to which they belong.

Prerequisites

- IP VPN Service Provisioning tool main window is open

Procedure steps

1 In the tree hierarchy of the Service Provisioning - IP VPN main window, select the VPN which contains the VRF to be excluded.

2 Right click on the VPN, and select **Manage VRFs...** from the pop-up menu.

The VRF Management dialog box opens.

3 From the VRF table at the top of the VRF Management dialog box, select the VRF that you wish to delete.

4 Click **Delete...**.

The Provisioning Options dialog box opens.

5 Activate the provisioning.

A progress dialog box shows the progress of the exclude VRF operation. Once successful, the VRF is removed from the VRF table.

If an error occurs while the operation is in progress, a message dialog box opens describing the error, the operation stops, and the tool disconnects from any node that it is connected to.

Procedure job aid

The following job aid provides information about possible error conditions:

Table 11
Possible error conditions when deleting a VRF

Error condition	Corrective action
Attempt to delete a VRF that has route targets belonging to multiple customers.	You have the option to either accept or decline to delete the VRF. If you accept, the IP VPN SP tool will remove the VRF from the selected VPN only. If you decline, you can cancel the procedure and just remove selected route targets. See “Removing a route target from a 2547 VPN” (page 77).

Modifying a 2547 VPN

Use the IP VPN SP tool to modify the VPN name, maximum access points, route target list, and description as required. This will update the VPN information in the Administration Database.

Prerequisites

- the VPN that you are modifying is stored in the database
- IP VPN Service Provisioning tool main window is open

Procedure steps

1 Select a 2547 VPN in the tree hierarchy in the Service Provisioning - IP VPN main window.

The **Apply** and **Cancel** command buttons are disabled.

2 Make the changes to any of the **VPN Name**, **Maximum Access Points**, **Route Target** list, and **Description** fields in the VPN Details panel.

The **Apply** and **Cancel** buttons become enabled.

3 Click **Apply**.

The status changes to Stored in the Administration Database.

Procedure job aid

The following job aid provides information about possible error conditions:

Table 12
Possible error conditions when modifying a 2547 VPN

Error condition	Corrective action
Warning to indicate that the route target is currently being used by VRFs in the VPN and cannot be deleted.	Remove the route target from each of the VRFs that use it. Otherwise, you can cancel the procedure and just remove selected route targets.

Viewing the VRF access details

View the active view for the VRF access on the Passport node.

Procedure steps

1. In the tree hierarchy of the Service Provisioning - IP VPN window, select and expand the customer object.

2. Right-click on the appropriate VPN name.

3. From the popup menu, select **Manage VRFs...**.

   The **VRF Management** dialog opens.The table at the top of the dialog displays a list of VRs that you have already added to the selected VPN.

4. From the VRF list, select the VRF you want to view.

   The VRF details are populated to the VRF Summary section.

5. Select the **VRF Access** tab.

6. In the bottom panel of the window, select the **Access Detail**s tab.

7. In the **Component to modify** picklist, select the component (Port, Media, Logical Interface, or Service Interface) that you want as the starting point for the IP VPN SP tool to load.

   The component tree hierarchy loads in the left panel of the Access Details.

8. Right-click on the component or attribute to open the popup menu and select **Display Provisionable** or **Display Operational**.

   The VRF access details display in the right panel.

Viewing the VRF details

View the active view for the VRF on the Passport node.

Procedure steps

1 In the tree hierarchy of the Service Provisioning - IP VPN window, select and expand the customer object.

2 Right-click on the appropriate VPN name.

3 From the popup menu, select **Manage VRFs...**.

The **VRF Management** dialog opens.The table at the top of the dialog displays a list of VRs that you have already added to the selected VPN.

4 From the VRF list, select the VRF you want to view.

The VRF details are populated to the VRF Summary section.

5 Select the **VRF Details** tab.

6 In the **Component to modify** picklist, select the component (OSPF, BGP, RIP Ext Policy, Diffserv, General VRF, or CAS) that you want as the starting point for the IP VPN SP tool to load.

The component tree hierarchy loads in the left panel of the VRF Details.

7 Right-click on the component or attribute to open the popup menu and select **Display Provisionable** or **Display Operational**.

The VRF details display in the right panel of the VRF Details.

Removing a route target from a 2547 VPN

Use the IP VPN SP tool to remove a route target from a 2547 VPN.

Prerequisites

- IP VPN Service Provisioning tool main window is open

Procedure steps

1 Select the 2547 VPN in the tree hierarchy of the IP VPN SP tool main window.

2 In the **Assigned Route Targets** section, select the route target that you want to delete.

3 To the right of the **Assigned Route Targets** section, click **Remove...**.

The route target is removed from the VPN Route Target Usage table.

4 Click **Apply** to remove the RT from the VPN.

If the RT is not used by any other VPN, it is also removed from the Administration Database.

Procedure job aid

The following job aid provides information about possible error conditions:

Table 13
Possible error conditions when removing a route target from a VPN

Error condition	Corrective action
Warning to indicate that the route target is currently being used by VRFs in the VPN and cannot be deleted.	Remove the route target from each of the VRFs that use it. Otherwise, you can cancel the procedure and just remove selected route targets.

Modifying a 2764 VPN

Use the IP VPN SP tool to modify the VPN name, private network address, and description, as required. This will update the VPN information in the Administration Database.

Prerequisites

- the VPN that you are modifying is stored in the database
- IP VPN Service Provisioning tool main window is open

Procedure steps

1. Select a 2764 VPN in the tree hierarchy in the Service Provisioning - IP VPN main window.

   The **Apply** and **Cancel** command buttons are disabled.

2. Make the changes to the **VPN Name**, **Private Network Address**, and **Description** fields in the VPN Details panel.

   The **Apply** and **Cancel** buttons become enabled.

3. Click **Apply**.

   The status changes to Stored in the Administration Database.

Viewing the VR Details

View the active view on the Passport for the VR.

Procedure steps

1. In the tree hierarchy of the Service Provisioning - IP VPN window, select and expand the customer object.

2. Right-click on the appropriate VPN name.

3. From the popup menu, select **Manage VRs...**.

   The **Virtual Router Management** dialog opens.The table at the top of the dialog displays a list of VRs that you have already added to the selected VPN.

4. From the VR list, select the VR you want to view.

   The VR details are populated to the VR Summary section.

5. Right-click the VR name to display the popup menu.

6. Select the component (OSPF, BGP, RIP, General VR, or CAS Root) that you want as the starting point for the IP VPN SP tool to load.

   The result displays in the left section of the VR Details panel.

7. Right-click on the component or attribute and select **Display Provisionable** or **Display Operational**.

   The result displays in the right section of the VR Details panel.

Deleting a VR from an existing 2764 VPN

Use the IP VPN SP tool to delete a VR from a 2764 VPN. You must delete all VRs before you can delete a VPN.

Prerequisites

- no access interfaces provisioned on the VR
- IP VPN Service Provisioning tool main window is open

Procedure steps

1. In the tree hierarchy of the Service Provisioning - IP VPN main window, select the VPN which contains the VR to be excluded.
2. Right click on the VPN, and select **Manage VRs...** from the pop-up menu.

   The Virtual Router Management dialog box opens.
3. From the VR table at the top of the Virtual Router Management dialog box, select the VR that you wish to delete.
4. Click **Delete...**.

   The Provisioning Options dialog box opens.
5. Activate the provisioning.

   A progress dialog box shows the progress of the exclude VR operation. Once successful, the VR is removed from the Virtual Routers table at the top of the VR Management dialog box.

   If an error occurs while the operation is in progress, a message dialog box opens describing the error, the operation stops, and the tool disconnects from any node that it is connected to.

Deleting an IP CoS Profile from a VR

Use the IP VPN SP tool to delete an IP CoS Profile through the IP CoS Editor.

Prerequisites

- no references to the IP CoS Profile by a VR
- the VR in the tree hierarchy of the Service Provisioning - IP VPN main window is selected
- the Virtual Router Management dialog is open

Procedure steps

1. In the IP CoS Profiles panel of the Virtual Router Management dialog box, open the IP Cos Editor by clicking the browse button **[...]** to the right of either the **Access IP CoS Profile** or **Core IP CoS Profile** list.

   The **Edit/View 2764 IP Class of Service** dialog box opens.

2. Select or type a name in the **Profile Name** list.

3. Click **Delete**.

   You are given a message to inform you if the delete was successful or not.

4. Click **Close** to close the IP CoS editor dialog and return to the Virtual Router Management dialog.

   The relevant CoS Profile field is now populated with the CoS profile that was current when you closed the IP CoS editor dialog.

Chapter 5
IP VPN service provisioning tool

The IP VPN service provisioning (SP) tool simplifies the tasks you perform to configure and administer RFC 2547 VPNs and RFC 2764 VPNs with autodiscovery enabled.

ATTENTION You cannot use the IP VPN Service Provisioning tool to configure VPNs on Passport 6000 nodes loaded with P7.0.x software.

If you configured the VPNs using other methods, you can run discovery and then use the IP VPN SP tool to administer the 2547 VPNs and the 2764 VPNs with autodiscovery enabled.

Prerequisites to using the IP VPN SP tool

- Information about the following prerequisites is provided in 241-6001-400 *Preside MDM Administration Database User Guide*:
  - Preside Multiservice Data Manager Administration Database must be configured and running.
  - PE Network object must be created in Administration Database.
  - PE Routers must be assigned to PE Network in Administration Database
  - understand the role of the Administration Database in VPN configuration and management

- If you configured the VPNs using other methods, see 241-6001-400 *Preside MDM Administration Database User Guide* for information about the discovery process and how to set up the PE network before you use the IP VPN SP tool to administer existing VPNs.

ATTENTION	Some changes you make to VPN information can trigger discovery and have a serious impact on the VPN ownership and network boundaries. See 241-6001-400 *Preside MDM Administration Database User Guide*, VPN Management for details about the impact of changes to VPN information.

Navigation

Tool fundamentals

The IP VPN SP Tool consists of the following software components:

- Java-based GUI client that communicates directly with the Administration Database and the end-to-end (ETE) server.
- VPN database tables which are part of the Administration Database

You can run multiple instances of the tool on one or more Preside Multiservice Data Manager workstations.

When you use the tool to configure and activate on-node data, the Administration Database information is updated to maintain the current view of the network. If you do not activate the configuration data, the Administration Database information is not updated because the current network view has not changed.

When you use the tool to enter administrative (off-node) data such as customer information, the data is entered to the Administration Database.

Capabilities

The IP VPN SP tool capabilities include the following:

- for 2547 VPN, provisioning:
    - VRFs
    - route distinguishers
    - route targets to VPNs
    - Export Policies
    - Local ATM access
    - any component associated with a VRF or VRF access media
    - any component/sub-component associated with local ATM access
- for 2764 VPN with auto-discovery enabled:
    - provisioning of VRs
    - provisioning of inter-VR tunnels between the VCGs and the customer VRs
    - defining the Core and Access IP CoS Profiles for the VRs in a VPN
    - creating and saving multiple IP CoS Policy Groups for the VRs in the Administration Database as IP CoS Profiles.
    - distributing IP routing information across a VPN by using Multiprotocol Border Gateway Protocol (MP-BGP-4)
    - creating VPNs that use the Route Reflector topology. The tool lets you specify which VRs in the VPN will be Route Reflectors.
    - creating VPNs that use the hub and spoke topology
- VPN management in the Administration Database including creating and deleting VRs/VRFs, VPNs, and customers, and modifying VPNs.
- routine provisioning on VRs/VRFs

IP VPN service provisioning tool user interface

The IP VPN SP tool is launched from the Preside Multiservice Data Manager toolset icon under **Configuration -> Passport Devices -> Service Provisioning -> IP VPN Service Provisioning**. When you launch the IP VPN SP tool a dialog box opens to prompt you to log in to the Administration Database. Once the login is successful, you can use the IP VPN SP tool.

ATTENTION	The IP VPN SP tool cannot function without a successful connection to the Administration Database.

The user interface consists of windows. Some of the windows are divided into panels. Some windows have tabs at the top of the window, or at the top of a panel. When you select a tab, you open another layer of the window or panel.

When you open the IP VPN SP tool, you start at the first level of the interface called the Service Provisioning - IP VPN window. This is referred to as the main window. The main window consists of the following sections:

- “Menu bar” (page 86) at the top of the main window
- “Tree hierarchy” (page 88) at the left of the main window
- “Details panel” (page 90) at the right of the main window
- “Command buttons” (page 96) at the bottom of the main window

Menu bar

The menu bar contains the following menus:

- “File” (page 86)
- “Edit” (page 87)
- “Options” (page 87)
- “Tools” (page 87)
- “Help” (page 88)

File

The file menu contains the Exit command. This command closes the Service Provisioning - IP VPN window and exits the IP VPN SP tool.

Edit

The content of the Edit menu changes depending on the item you have selected in the tree hierarchy. The Edit menu content is identical to that of the popup menu you see when you right-click on the item in the tree hierarchy.

Options

The **Options** menu contains the following options:

- **Set Default Authentication..**.
  Selecting this option opens a dialog box that enables you to set a default userid and password for connecting to a PE node. When you exit the IP VPN SP tool, the userid and password are deleted.
- **Clone VR on Creation**
  The Clone VR on Creation option is enabled for 2764 VPNs only. When you click on the check box, you can clone an existing VR when adding a new VR to the customer VPN.
- **Clone VRF on Creation**
  The Clone VRF on Creation option is enabled for 2547 VPNs only. When you click on the check box, you can clone an existing VRF when adding a new VRF to the customer VPN.
- **Force VPN reload on customer expansion**
  Selecting this option enables the IP VPN SP tool to reload the VPN data that you have configured for a customer each time you click on the + sign beside the customer name in the tree hierarchy.
- **Warn when including External RTs**
  Selecting this option enables a warning message when you change an RT and the change will result in external access to the VPN.

Tools

The tools menu contains a launch point for the Frame Relay Service Provisioning (FR SP) tool. You use the FR SP tool to configure the VPN access between the customer site and the PE node for the following interface types:

- RFC 2547 IP Optimized Backhaul or Local
- RFC 2764 IP Optimized Backhaul or Local
- RFC 2764 FrDTE Backhaul or Direct

Help

The Help menu contains the Help on Window command. When you select this command, the internet browser is launched and the 241-6001-616 *Preside MDM IP VPN Service Configuration User Guide* is loaded to display the information about the IP VPN Service Provisioning tool.

Tree hierarchy

The tree hierarchy is the left panel of the IP VPN SP main window. When you start the IP VPN SP tool, the tree hierarchy displays the customer VPN data retrieved from the Administration Database when you ran autodiscovery. The customers that exist in the Administration Database are displayed in the tree hierarchy. If there are no user-defined customers in the Administration Database, then only the Default customer and the Service Provider customer are displayed in the tree hierarchy.

When an item in the tree hierarchy has sub-items, a plus (+) sign displays to the left of the item name. You click the + sign to expand or collapse the sub-items.

A + sign could also be displayed if it is the first time a Customer item is being expanded. If there are no VPNs for the Customer, then the + sign disappears after you attempt to expand the item.

Selecting and right-clicking on items and sub-items in the tree hierarchy displays a popup menu with options to allow to perform configuration tasks and access help information.

When you configure an item in the tree hierarchy and click the Apply button at the bottom of the window, the item is added to the Administration Database. If the item is a VR/VRF, it is also provisioned on the node.

All Customers menu

All Customers is the top level item in the tree hierarchy. When you select and right-click on this item, you have three options in the popup menu:

- **Add new customer**
  Select this option to add a new customer to the Administration Database.

- **Refresh**
  A Refresh of a specific Customer item reloads its respective VPNs from the Administration Database. A Refresh of the All Customers item reloads only the Customers from the Admin DB and collapses the items. Then when a Customer item is expanded, its VPNs are reloaded from the Administration Database.
- **Help**

Customer/<customer name> menu

Customer/<customer name> is the second level in the tree hierarchy. When you launch the IP VPN SP tool, there are always two customer names at this level: the Customer/Default customer and the Customer/Service Provider. The Default customer icon has a **D** superimposed on it. The Service Provider customer icon has an **SP** superimposed on it.

Existing customers that have been populated to the Administration Database or that you have added using the IP VPN SP tool are also displayed at this level in the tree hierarchy, with plain icons. When you select and right-click on a customer name, you have four options in the popup menu:

- **Add new 2764 VPN**
  Select this command to add a new 2764 autodiscovery mode VPN to the selected customer.
- **Add new 2547 VPN**
  Select this command to add a new 2547 VPN to the selected Customer.
- **Delete**
  The Delete command lets you delete a Customer from the Administration Database and from the tree hierarchy. You can only delete a Customer if it has no references to circuits or VPNs in the database.
- **Refresh**
  The Refresh command lets you reload the VPNs (2764 and 2547) to the tree hierarchy for the selected Customer.

VPN menu

<RFC>_<vpn name> is the third level in the tree hierarchy

ATTENTION	Any 2764 VPN with autodiscovery enabled that was configured without the IP VPN SP tool is displayed under the Default Customer. You must re-assign these VPNs to the appropriate customer entities in the database. See 241-6001-400 *Preside MDM Administration Database User Guide*.

When you select and right-click on a VPN, you have two options in the popup menu:

- **Manage VRs...**/**Manage VRFs...**.
  Select this command to open the Virtual Router Management/VRF Management dialog to add or modify a VR/VRF in the VPN. This menu option is available only if the selected VPN has been applied to the Administration Database.
- **Delete**
  If the VPN has been applied to the Administration Database, the Delete command removes the selected VPN from the database and updates the necessary tables. This operation succeeds only if the VPN has no VRs/ VRFs associated with it. If the VPN has not yet been applied to the database, the Delete operation only deletes the VPN from the tree hierarchy.

Details panel

The Details panel is the right side of the IP VPN SP main window. You use the Details panel to enter the configuration data or to view the existing data for the item you select in the tree hierarchy. The status of a selected item in the tree hierarchy is displayed at the bottom of the Details panel.

Three different status statements may be displayed:

- Stored in the Administration Database
- Not yet stored in the Administration Database
- Pending changes are not yet stored in the Administration Database

The Details panel is blank when you select the All customers item from the tree hierarchy. When you select any other item in the tree, the IP VPN SP tool displays the data relating to the selection in the relevant fields. If there is no data in the Administration Database, the field data is blank.

If you make changes in the Details panel and then click outside the panel before you have saved the changes, you will be prompted to return and save the changes or lose the changes that have been made. If you have not saved the changes, you can cancel the changes at any time by clicking on the Cancel button.

Tool tips are available for entries in the Details panel. The tool tip text displays the valid values and ranges for the entry field. To access the tool tip, rest the mouse pointer over the entry field for two seconds.

For information about the fields in the Details panel for the Customer, 2764 VPN, and 2547 VPN, see the following tables:

- “Details panel for customer” (page 91)
- “Details panel for 2547 VPN” (page 92)
- “Details panel for 2764 VPN” (page 94)

Details panel for customer

Table 14
Details panel for Customer

Field	Description	Valid value or range
Customer Name	Customer name	Determined by the Administration Database. Spaces are allowed.
Default Customer check box	Check box indicating if the customer is the default customer. The Administration Database contains one default customer	This is a read-only field.
(Sheet 1 of 2)		

Table 14 (Continued)
Details panel for Customer

Field	Description	Valid value or range
Service Provider check box	Check box indicating if the customer is a service provider customer. The Administration Database contains one Service Provider Customer.	This is a read-only field.
Description (optional)	An editable field for entering a description of the customer.	Up to 2000 characters.
(Sheet 2 of 2)		

Details panel for 2547 VPN

Table 15
Details panel for 2547 VPN

Field	Description	Valid value or range
VPN name	Name of the VPN.	Determined by the Administration Database. Spaces are allowed.
VPN type	RFC type of the VPN.	2547. This is a read-only field.
Max. Access Points	The sum of all the access interfaces on all the VRFs in the selected VPN.	An integer value
PE Network Name	Select a PE Network name from a pick list containing the names of the PE networks you have added to the Administration Database	
Assigned Route Targets	A table of the route targets that have been added to the VPN. An RT must be in this table before a VRF in the VPN can include the RT. Indicate whether the RT is Extranet for either of the following conditions: • the customer that owns the VPN does not own the RT • the RT is included in another VPN owned by another customer	The RT can be in either of the following formats: • <AS>:<assigned value> • <IP>:<assigned value>
(Sheet 1 of 2)		

Table 15 (Continued)
Details panel for 2547 VPN

Field	Description	Valid value or range
Add... button	Opens the Manage Route Target dialog box to enable you to specify a Route Target to add to the Route Targets table or to generate a new Route Target. See “Manage route targets for 2547 VPN” (page 93).	
View/Edit... button	Opens the Manage Route Targets dialog to enable you to change the RT description and owner. See “Manage Route Targets for 2547 VPN” (page 93)	
Remove button	Removes the selected Route Target from a VPN. If this RT is no longer used by any other VPN, it is deleted from the Administration Database.	
Show Extranet VPNs...	Opens the Route Target usage dialog which lists all other VPNs and their associated customers, that are using this Route Target.	
Description field (optional)	A text description for the VPN.	Up to 2000 characters.
(Sheet 2 of 2)		

Manage Route Targets for 2547 VPN

Table 16
Manage route targets for 2547 VPN

Field	Description	Valid value or range
Route Target	Manually enter the Route Target to be added to the customer VPN.	
Generate RT	Click this button to automatically generate a Route Target to be added to the customer VPN.	
Browse...	Click this button to open the All Route Targets dialog where you can select an existing Route Target to add to the VPN.	
(Sheet 1 of 2)		

Table 16 (Continued)
Manage route targets for 2547 VPN

Field	Description	Valid value or range
RT Owner	The Route Target owner. If the RT is extranet to the VPN, the RT Owner will be different from the VPN customer. If you change the RT Owner, and click Apply in the VPN Details dialog box, discovery automatically runs. NOTE: If you modify the RT ownership so that two of the customer VPNs have the same RT, the VPNs will be merged.	
Description (optional)	A text description for the Route Target.	If you launched this dialog from the View/Edit... and picked a different owner from the RT Owner list, discovery updates the description to indicate the change.
(Sheet 2 of 2)		

Details panel for 2764 VPN

Table 17
Details panel for 2764 VPN

Field	Description	Valid value or range
VPN name	Name of the VPN	Determined by the Administration Database. Spaces are allowed.
VPN type	RFC type of the VPN.	2764. This is a read-only field.
(Sheet 1 of 2)		

Table 17 (Continued)
Details panel for 2764 VPN

Field	Description	Valid value or range
VPN Identifier	Unique VPN identifier	This is a dashed 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 4-digit pairs represent the 4-octet VPN index. Example: 11-12-12-14-15-16-17
AS ID	Autonomous System Identifier for BGP routing	Integer.
Private Network Address	VPN Private Address.	The Private Network Address. The format is <ip address>/<mask>. The mask for the Private Network Address is an integer from 0 to 32, in accordance with the Classless Inter-Domain Routing (CIDR) addressing scheme for allocating IP addresses.
PE Network Name	Select a PE Network name from a pick list containing the names of the PE networks you have added to the Administration Database	
Description (optional)	Enter a text description for the VPN	Up to 2000 characters.
Enable Multi-Protocol BGP check box	Check this box to indicate that the VPN supports MP-BGP.	
(Sheet 2 of 2)		

Command buttons

Use the command buttons at the bottom of the Details panel to perform the following operations:

- **Delete**
  Click this button to delete the selected item from the Administration Database.
- **Apply**
  Click this button to complete the data entry and update the Administration Database information.
- **Cancel**
  Cancel what you have entered in the Details panel at any time BEFORE you click the Apply button.

VRF Management dialog

When you select and right-click a 2547 VPN from the tree hierarchy, you can select Manage VRF... from the popup menu. This opens the VRF Management Dialog so you can add and configure the VRFs for the customer VPN. The VPN name is displayed in the dialog box title.

The VRF Management dialog consists of two main sections:

- “Node and VRF table” (page 96) at the top of the dialog
- “VRF Summary tab” (page 96), “VRF Details tab” (page 100), and “VRF Access tab” (page 100) at the bottom of the dialog.

Node and VRF table

This table contains list of the VRFs that belong to the selected VPN, and their associated PE nodes. This list is updated dynamically as you add new VRFs to the VPN. When you select a VRF from this table, the fields in the VPN Routing Function Details are automatically populated with the related data. See “VRF Summary tab” (page 96).

VRF Summary tab

You enter configuration information about the VRF in the VRF Summary fields. The fields are divided into groups and displayed in group boxes.

For information about the groups and their respective fields, see “VRF Summary details for 2547 VPN” (page 97).

Table 18
VRF Summary details for 2547 VPN

Group	Field	Description	Valid value/range
Node	Node Name	Select the node on which the VRF will be created.	The list of nodes displayed contains only those that belong to the PE Network that you selected when you created the VPN.
	Use Defaults check box	Check this box to use the default userid and password to log on the PE node. Otherwise, enter userid and password to override the default values.	
(Sheet 1 of 3)			

Table 18
VRF Summary details for 2547 VPN

Group	Field	Description	Valid value/range
VRF	VRF Name or ...	Enter the name of the VRF or click the **...** button to select a name from the Common VRFs for Node dialog box. This lists all VRFs under the PE Router on the specified node. See “Common VRFs for the node” (page 99).	Must be the same name as provisioned on the node.
	Description	Enter a description that will be stored in the Administration Database.	Up to 2000 characters.
	Route Distinguisher	Enter the RD that uniquely identifies the same private ipv4 addresses that belong to different VPNs. The RD configured for the VRF must be unique within the PE for all the VRFs. NOTE: If you change the RD value, BGP withdraws all the routes learned by the VRF from its peers and flushes the routes from the Routing Information Base (RIB). BGP re-installs the routes in the VRF into the RIB and re-announces the routes with the new RD value. BGP also installs any already learned routes destined to that VRF in the VRFs routing database.	The RD can be in either of the following formats: • <AS>:<assigned value> • <IP>:<assigned value>
	Description	Enter a description that will be stored in the Administration Database.	Up to 2000 characters.
PE Network	PE Network Name	The PE network name that the VPN belongs to.	This is a read-only field associated with the selected node.
	PE Router	The name of the PE Router provisioned on the node.	This is a read-only field associated with the selected node.
(Sheet 2 of 3)			

Table 18
VRF Summary details for 2547 VPN

Group	Field	Description	Valid value/range
Route Targets	Available RTs in this VPN	A table of the Route Targets and customer names associated with the VPN. Select an RT to activate the action buttons **Add RT to VRF** and **Show VRFs Common to RT...**.	
	<action buttons>	Select a Route Target from the list of **Available RTs in the VPN** and click the action button **Add RT to the VRF**, or **Show the VRFs Common to RT...**. Select a Route Target from the list of **Selected RTs in Current VRF** and click the action button **Remove RT from VRF**.	
	Selected RTs in current VRF	Lists the RTs that you have added to the VRF and their respective import/export mode. Select an RT to activate the action button **Remove RT from VRF...**.	
(Sheet 3 of 3)			

Common VRFs for the node

Table 19
Common VRFs for the node

Field	Description	Valid value or range
Node	The name of the node that was selected in the **Node Name** field VRF Management dialog.	This is a read-only field.
VRF	The list of the VRFs that have been configured on the node. Select a VRF to populate the **VRF Name** field of the VRF Management dialog.	

VRF Details tab

The tab is enabled if you select a VRF from the Node and VRF table. This opens a list of components that you select as the starting point for the IP VPN SP tool to load into the VRF Details panel. The IP VPN SP tool queries the PE node and loads the component model from the active view. The components and attributes from that starting point display in the left side of the VRF Details panel.

You can right-click on each component to open a popup menu. Select either Provisionable or Operational to display the respective attributes in the right side of the VRF Details panel. You may also add, modify, or delete sub-components by selecting the appropriate item from the popup menu..

VRF Access tab

You select the VRF Access tab to view the existing local ATM access to the customer site and optionally modify the access. The tab is enabled only if you successfully add a VRF to the 2547 VPN.

The top part of the VRF Access tab contains a table of provisioned local ATM access methods for the selected VRF. You can browse through this table to select the method to use for the new access.

The bottom part of the tab contains two additional tabs:

- “Access Summary tab” (page 100)
- “Access Details tab” (page 101)

Access Summary tab

You use the VRF Access Summary to configure the local ATM access method. Once the access is configured, it appears in the top part of the VRF Access panel.

For information about the fields in the access summary, see “VRF Access Summary for Local ATM” (page 101).

Table 20
VRF Access Summary for Local ATM

Field	Description	Valid value or range
Access Type	A pick list of access methods.	Local ATM
Site	Enter the site for the access point or browse for an existing site by clicking on the **...** button beside the Site field.	ASCII string of up to 128 characters.
Port	A pick list of the existing unassigned port interfaces. Select one for the access method.	
AtmIf	Enter the instance of the on-node AtmIf component.	An integer from 1 to 4095.
VCC table	Enter up to 4 VCC entries to correspond with the relevant class service.	
Access Point	Enter a name to use for the access interface or click on the Use Logical Interface checkbox.	Up to 128 characters or read-only if click Use Logical Interface checkbox.
Use Logical Interface checkbox	Optionally click this checkbox to use the IP Logical Interface address as the name of the access point. The Access Point field will be populated with the same IP address that you enter in the Logical Interface field.	
Logical Interface	Enter the address of the logical interface.	<IP address>/<network mask>

Access Details tab

Use the Access Details tab to add, modify, or delete subcomponents for the access method you create in the Access Summary. The Access Details tab consists of a component hierarchy on the left of the tab and the Provisionable and Operational attributes displayed on the right.

In the Access Details, Component to Modify field, select the component that you want to work with. Once the component tree is loaded into the left panel, right-click the component to open a popup menu. Select Add, Delete, or Modify.

If you add a subcomponent, it is added to the component hierarchy with bold font. If you delete a component or subcomponent that is shown in the hierarchy, the font is greyed. The changes to the font style indicate that the addition/deletion has not yet been applied on the node. In addition, an icon shows next to the component or subcomponent to indicate that it is newly added or deleted.

If you select Modify from the popup menu, a dynamic form opens with all the provisionable attributes that you can modify for the selected component. When you modify the component, the component font is bolded and is marked with an icon to indicate that it is newly modified and that the change has not been applied on the node.

When you have completed modifying the component hierarchy, you click Apply to open the Provisioning Options dialog and activate the changes on the node. When activation is successful, the component colors change to black and the icons are removed to indicate that the changes have been applied to the node.

Command buttons

Use the command buttons at the bottom of the Details panel to perform the following operations:

- **New**
  Click this button to enter the data for a new VRF in the selected VPN. If you want to clone an existing VRF, select the VRF from the Node and VRF table and then click the New button. See “Adding a VRF by cloning” (page 41).
- **Delete**
  Click this button to delete the selected VRF from the Administration Database and remove the VRF provisioning from the node.
- **Apply**
  Click this button to complete the data entry. A dialog box prompts you to either activate or save the data on the node.

ATTENTION	If you do not activate the data on the node, the VRF data is not written to the Administration Database.

- **Cancel**
  Cancel what you have entered in the Details panel at any time BEFORE you click the Apply button.
- **Close**
  Click on this button to close VRF Management dialog and return to the VPN details.
- **Help**
  Click on this button to launch information about the fields in the VRF Management dialog.

Virtual Router Management dialog

When you select and right-click a 2764 VPN from the tree hierarchy, you can select Manage VR... from the popup menu. This opens the Virtual Management dialog so you can add and configure the VRs for the customer VPN. The VPN name is displayed in the dialog box title.

The Virtual Router Management dialog consists of two main sections:

- “Node and Virtual Router table” (page 103) at the top of the dialog
- “VR Summary tab” (page 103) and “VR Details tab” (page 108) at the bottom of the dialog

Node and Virtual Router table

This table contains list of the VRs that belong to the selected VPN, and their associated PE nodes. This list is updated dynamically as you add new VRs to the VPN. When you select a VR from this table, the VR Summary fields are automatically populated with the related data. See “VR Summary tab” (page 103).

VR Summary tab

You select the VR Summary tab to display the fields that you use to configure the VR. The fields are divided into groups and displayed in group boxes.

For information about the groups and their respective fields, see “VR Summary for a 2764 VPN” (page 104).

Table 21
VR Summary for a 2764 VPN

Group	Field	Description	Valid value/range
Node	Node Name	PE node that is the access for the VPN customer site.	
	Use Defaults check box	Check this box to use the default userid and password to log on the PE node. Otherwise, enter userid and password to override the default values.	
PE Network	PE Network Name	The PE network name that the VPN belongs to.	
	Virtual Carrier Gateway	The name of the VCG that you have provisioned on the PE node.	This is a read-only field.
Inter-VR Tunnel	Private Logical Interface	This corresponds to the IP address for the logical interface on the customer VR.	IP address/netmask where the netmask is a value from 0 to 32.
	IP Aggregation Enable Public IP Aggregation check box	Check this box to enable you to enter data in the Public Logical Interface and Public Source End Point fields.	
	IP Aggregation Public Logical Interface	This value corresponds to the IP Logical Address on the VCG. You can enter data in this field only if you have checked the Enable Public IP Aggregation box.	IP address/netmask where the netmask is a value from 0 to 32.
	IP Aggregation Public Source End Point	This value corresponds to the source address of the PTMP tunnel for the customer VR and is within the same network address space as the Public Logical Interface. You can enter data in this field only if you have checked the Enable Public IP Aggregation box at the VPN level.	IP address
(Sheet 1 of 3)			

Table 21
VR Summary for a 2764 VPN

Group	Field	Description	Valid value/range
Virtual Router	Virtual Router Name	Name of the VR	Must be the same name as provisioned on the node.
IP CoS Profiles	Access IP CoS Profile	Select None or select the IP CoS profile for the CE-PE interface. Otherwise, click on the **...** button to launch the IP CoS Profile Editor. See “Edit/View 2764 IP Class of Service” (page 106).	
	Core IP CoS Profile	Select None or select the IP CoS profile for the PE to PE interface. Otherwise, click on the **...** button to launch the IP CoS Profile Editor. See “Edit/View 2764 IP Class of Service” (page 106).	
(Sheet 2 of 3)			

Table 21
VR Summary for a 2764 VPN

Group	Field	Description	Valid value/range
Routing	BGP Route Reflector check box	Check this box if the VR is a route reflector.	
	BGP Hub check box	Check this box if the VR is the hub of a fully-meshed PE network.	
	BGP Spoke check box	Check this box if the VR is a spoke in a fully-meshed PE network.	
	Multi-Protocol BGP MBGP Route Reference	An on-node attribute. This field is enabled only if you have checked the Enable Multi-Protocol BGP check box in the VPN Details panel.	An integer value from 1 to 253.
	Multi-Protocol BGP Import Route Limit	The maximum number of MBGP routes that can be imported from VCG BGP Ribin. This field is enabled only if you have checked the Enable Multi-Protocol BGP check box in the VPN Details panel.	An integer value from 1 to 65535.
	Multi-Protocol BGP Export Route Limit	The maximum number of customer VR routes that can be exported into VCG BGP Ribin. This field is enabled only if you have checked the Enable Multi-Protocol BGP check box in the VPN Details panel.	An integer value from 1 to 65535.
(Sheet 3 of 3)			

Edit/View 2764 IP Class of Service

You launch the IP CoS Editor from the VR Summary window. For each VR you add, there are popup menus for the two types of 2764 IP CoS profiles: Access and Core. These profiles are applied to the node when you apply the rest of the VR information to the node.

The IP CoS profiles are stored in the Administration Database.You can store multiple 2764 IP CoS profiles in the Administration Database and create new ones by selecting an existing profile and changing the relevant parameters. When you save the changes a new version of the profile is created using the base profile name and the new version number.

You can only delete an IP Cos profile if it is not referenced by a customer VR.

For information about the IP CoS Editor fields, see “Edit/view 2764 IP Class of Service” (page 107).

Table 22
Edit/view 2764 IP Class of Service

Field	Description	Valid value/range
Profile Name	The Profile name that was selected in the VR Summary when the user launched the IP CoS Editor. If None was selected, then this field is blank.	Dependent on selection in VR Summary window.
Description	Enter a description that will be stored in the Administration Database.	Free flow text.
ToS Markings	Map ToS to CoS values 0 to 3.	A 2-digit hex value.
ToS Mask	Enter the ToS mask number.	A 2-digit hex value.
CoS Policies	List of CoS policies that are present in the Administration Database. Select policy and click appropriate button to modify or delete. Otherwise, click the Add... button to add a new policy. See “Add new CoS Policy for 2764 VPN” (page 108).	

Add new CoS Policy for 2764 VPN

Table 23
Add new CoS Policy for a 2764 VPN

Field	Description	Valid value/range
Policy	Enter the CoS policy number.	Range from 1 to 20 ASCII characters.
CoS Index	Enter the CoS index number.	Range from 0 to 3.
ToS Map	Enter the ToS map number.	List of space-separated ToS hex values.
Flow Classification	The instance of the IPAddrLayer4Flow attribute on the VR component. See “Flow classification attributes for CoS policy” (page 108)	Must be the same as provisioned on the node attribute: Vr/<instance> IP Pg/ <instance> Policy/ <instance> **IPAddrLayer4Flow/ <instance>**

New Flow Classification for CoS policy

Table 24
Flow classification attributes for CoS policy

Field	Description	Valid value/range
Flow Classification Identifier	The flow classification ID.	1 to 1023
Protocol	The protocol type.	TCP, UDP, or ICMP
Port	The port number.	0 to 65535
Prefix	The prefix.	IP Address
Prefix Length	The prefix length.	0 to 32

VR Details tab

You use the VR Details tab to view or configure VR components and attributes. The tab is enabled only if you select a VR from the Node and Virtual Router table and right-click. This opens a list of components that you select as the starting point for the IP VPN SP tool to load into the VR Details panel. The IP VPN SP tool queries the PE node and loads the component model from the active view. The components and attributes from that starting point display in the left side of the VR Details panel.

You can right-click on each component to open a popup menu. Select either Provisionable or Operational to display the respective attributes in the right side of the VR Details panel.

Command buttons

Use the command buttons at the bottom of the Details panel to perform the following operations:

- **New**
  Click this button to enter the data for a new VR in the selected VPN. If you want to clone an existing VR, select the VR from the Node and VR table and then click the New button. See “Adding a VR by cloning” (page 60).
- **Delete**
  Click this button to delete the selected VR from the Administration Database and remove the VR provisioning from the node.
- **Apply**
  Click this button to complete the data entry. A dialog box prompts you to either activate or save the data on the node.

ATTENTION	If you do not activate the data on the node, the VR data is not written to the Administration Database.

- **Cancel**
  Cancel what you have entered in the Details panel at any time BEFORE you click the Apply button.
- **Close**
  Click on this button to close Virtual Router Management dialog and return to the VPN details.
- **Help**
  Click on this button to launch information about the fields in the Virtual Router Management dialog.

Chapter 6 IP VPN provider edge provisioning tool

The IP VPN provider edge provisioning (PEP) tool simplifies the tasks you perform to configure the BGP peers in a provider edge (PE) network so that you can configure RFC 2547 IP VPN service for your customers.

If you configured the BGP peers using other methods, you can run discovery and then use the IP VPN PEP tool to administer existing BGP peers in the PE network.

Prerequisites to using the IP VPN PEP tool

- Information about the following prerequisites is provided in 241-6001-400 *Preside MDM Administration Database User Guide*:
  - — Preside Multiservice Data Manager Administration Database must be configured and running.
  - — PE Network object must be created in the Administration Database.
- If you configured the BGP peers using other methods, see 241-6001-400 *Preside MDM Administration Database User Guide* for information about the discovery process and how to set up the PE network before you use the IP VPN PEP tool to administer existing BGP peers.

Navigation

Tool fundamentals

The IP VPN PEP tool is launched from the Preside Multiservice Data Manager toolset icon under **Configuration -> Passport Devices -> Service Provisioning -> IP VPN PE Provisioning**. When you launch the IP VPN PEP tool, the tool opens in disabled mode. Then a dialog box opens to prompt you to log in to the Administration Database. Once the login is completed, the IP VPN PEP tool is enabled.

Capabilities

The IP VPN PEP tool capabilities include the following:

- creating the PE network object in the Administration Database
- adding/removing peering relationships in a fully-peered mesh network
- configuring the Passport side of the peer setup when adding a Foreign node to a fully-peered mesh network
- configuring the Passport side of a peering relationship in a route reflector network
- looking up the primary loopback address to be used when configuring the peering relationships

Administration Database requirement

The IP VPN PEP tool uses the Administration Database for its data storage requirements. Each time a user successfully creates an IP VPN related component, database objects are created in the Administration Database. The database contains additional data related to the IP VPN that only exists off-switch. Off-switch data includes such items as the PE Network.

The Administration Database enables the IP VPN PEP tool to collect and store data for 2547 Provider Edge Networks.

IP VPN PEP tool user interface

The IP VPN PEP tool provides a user interface to enable you to access the tool and configure the BGP peers in the PE network.

The user interface is a window that contains the following sections:

- "Menu bar" (page 113) at the top of the window
- "Tree Hierarchy" (page 114) at the left of the window
- "Details panel" (page 116) at the right of the window
- "Command buttons" (page 120) at the bottom of the window

Menu bar

The menu bar contains the following menus:

- "File" (page 113)
- "Edit" (page 113)
- "Options" (page 113)
- "Tools" (page 114)
- "Help" (page 114)

File

The file menu contains the Exit command. This command closes the Service Provisioning - IP VPN window and exits the IP VPN PEP tool.

Edit

The content of the Edit menu changes depending on the item you have selected in the tree hierarchy. The Edit menu content is identical to that of the popup menu you see when you right-click on the item in the tree hierarchy. See "Tree Hierarchy" (page 114).

Options

The **Options** menu contains the following one option:

- **Authentication..**.
  Selecting this option opens a dialog box that enables you to set a default user ID and password for connecting to a PE node.

Tools

The tools menu contains two options that provide launch points for

- IP VPN SP tool
- Nodal Provisioning (NP) tool

Help

The Help menu contains the Help on Window command. When you select this command, the internet browser is launched and the 241-6001-616 *Preside MDM IP VPN Service Configuration User Guide* is loaded to display the information about the IP VPN Provider Edge Provisioning tool.

Tree Hierarchy

The tree hierarchy is the left panel of the IP VPN PEP main window. When you start the IP VPN PEP tool, the tree hierarchy displays the PE Network data retrieved from the Administration Database. If there are no PE Network objects in the Administration Database, then only the All PE Networks item is displayed in the tree hierarchy.

When an item in the tree hierarchy has sub-items, a plus (+) sign displays to the left of the item name. You click the + sign to expand or collapse the sub-items.

A + sign could also be displayed if it is the first time a PE Network item is being expanded.

Selecting and right-clicking on the items and sub-items in the tree hierarchy displays a popup menu with options to allow to perform configuration tasks and access help information.

When you configure an item in the tree hierarchy, it is only added to the Administration Database, and where applicable, provisioned on the node, when you click the Apply button at the bottom of the main window. See “Command buttons” (page 120).

All PE Networks menu

All PE Networks is the top level item in the tree hierarchy. When you select and right-click on this item, you have one option in the popup menu:

- Create PE Network
  Select this option to add a new PE Network element to the Administration Database. (You can also add a new PE Network element using the Administration Database tool.)

<PE network name> menu

<PE Network name> is the second level in the tree hierarchy.

When you select a PE network with a fully-peered topology and right-click you have one option in the popup menu:

- **Add Router**
  Select this command to add a new PE Router to the selected PE Network.

When you select a PE network with a route reflector topology and right-click you have two options in the popup menu:

- **Add Router**
  Select this option to add a new PE Router to the selected PE Network.
- **Add Router Reflector**
  Select this option to add a new route reflector to the selected PE Network.

ATTENTION A Passport with PCR 5.2 cannot act as a route reflector in a 2547 PE network.

PE Router menu

<router type>/<router name> is the third level in the tree hierarchy

If the PE Network is a fully-peered mesh topology, the router type is always non-route reflector. This is indicated by router type Rtr.

When you select a PE router in a fully-peered PE network and right-click you have one option in the popup menu:

- **Delete Peering**
  Select this command to delete a PE Router from the selected fully-peered network.

If the PE Network is a route reflector topology, some of the routers are designated as route reflectors. This is indicated by router type RR. All the routers that are non-route reflectors are indicated by router type Rtr.

When you select a PE router of router type RR in a route reflector network and right-click, you have one option in the popup menu:

- **Delete Peering**
  Select this command to delete the PE Router that is the route reflector from the selected route reflector network.

When you select a PE router of router type Rtr in a route reflector network and right-click you have one option in the popup menu:

- **Delete Peering**
  Select this command to delete a PE Router that is not the route reflector from the selected route reflector network.

Details panel

The Details panel is the right side of the IP VPN PEP main window. You use the Details panel to enter the configuration data or to view the existing data for the item you select in the tree hierarchy. The status of a selected item in the tree hierarchy is displayed at the bottom of the Details panel.

The following status statements may be displayed:

- Changes are pending
- Applied

The Details panel is blank when you select the All PE Networks item from the tree hierarchy. When you select any other item in the tree, the IP VPN PEP tool displays the data relating to the selection in the relevant fields. If there is no data in the Administration Database, the field data is blank.

If you make changes in the Details panel and then click outside the panel before you have saved the changes, you will be prompted to return and save the changes or lose the changes that have been made. If you have not saved the changes, you can cancel the changes at any time by clicking on the Cancel button.

Tool tips are available for entries in the Details panel. The tool tip text displays the valid values and ranges for the entry field. To access the tool tip, position the cursor over the entry field for two seconds.

For information about the fields in the Details panel for the PE Network and PE Router, see the following tables:

- “Details panel for PE Network” (page 117)
- “Details panel for PE router in a fully peered mesh network” (page 118)
- “Details panel for PE router in a route reflector network” (page 119)
- “Details panel for route reflector” (page 120)

Details panel for PE Network

Table 25
Details panel for PE Network

Field	Description	Valid value or range
PE Network	PE Network name	Determined by the Administration Database. Spaces are allowed.
Autonomous System Number	Autonomous System Number for BGP peering.	A value in the range 0...65535
Topology	List for selecting for the PE Network topology type.	Fully Peered Mesh or Route Reflector
Description (optional)	An editable field for entering a description of the PE network.	Up to 2000 characters.

Details panel for PE router in a fully peered mesh network

Table 26
Details panel for PE router in a fully peered mesh network

Field	**Description**	**Valid value or range**
Node Type	List for selecting the node type.	**Passport** or **Foreign**.
Node Name	If the node type is **Passport**, this field is a list of all the Passport nodes that are found in HGDS. Select the node or begin typing. The box will autofill with the node name. If the node type is foreign, enter the name to be used to represent the node in the Administration Database.	If the node type is **Foreign** this is a free-flow text field used for Administration Database only.
Create Router Component...	Launches the Nodal Provisioning tool for adding a router component to the node if none exists.	
Router Name	For a Passport node, this field will autofill with the node name and the router instance when the user clicks the Apply command button. See “Command buttons” (page 120). For a foreign node, type in a router name to be used in the Administration Database.	If the node type is **Passport** node, this field is read-only. If the node type is **Foreign** this is a free-flow text field used for Administration Database only.
Primary Loopback Address	For a Passport node, this field will autofill when the user clicks the Apply command button. See “Command buttons” (page 120). For a Foreign node, type in the primary loopback address.	If the node type is **Passport**, this field is read-only. If the node type is **Foreign**, use only IP address format.
Description (optional)	An editable field for entering a description of the PE router.	Up to 2000 characters.

Details panel for PE router in a route reflector network

Table 27
Details panel for PE router in a route reflector network

Field	Description	Valid value or range
Node Type	List for selecting **Passport** to indicate the node type.	**Passport** is the only value
Node Name	List of all the Passport nodes that are found in HGDS. The box will autofill as the user types into it.	
Create Router Component...	Launches the Nodal Provisioning tool to add a router component to the node if none exists.	
Router Name	A field that will autofill with the node name and the router instance when the user clicks the Apply command button. See “Command buttons” (page 120).	Read-only
Primary Loopback Address	A field that will autofill when the user clicks the Apply command button. See “Command buttons” (page 120).	Read-only
Description (optional)	An editable field for entering a description of the PE router.	Up to 2000 characters.
Route Reflector list	List of available route reflectors for the PE network retrieved from the Administration Database. Click on the appropriate check box to select the route reflectors to be peered with the new router. NOTE: These node types are always **Foreign** for RFC 2547 and are not provisioned by the IP VPN PEP tool.	

Details panel for route reflector

Table 28
Details panel for route reflector

Field	Description	Valid value or range
Node Type	select **Foreign** to indicate the node type.	**Foreign** is the only value.
Router Name	Enter a router name to be used in the Administration Database.	Free-flow text. used for Administration Database only.
Node Name	Enter a node name to be used in the Administration Database.	Free-flow text. used for Administration Database only.
Primary Loopback Interface	The IP address of the always up interface on the router. This is the IP address that is used when setting up peering relationship.	IP address format.
Description (optional)	An editable field for entering a description of the PE router.	Up to 2000 characters.

Command buttons

Use the command buttons at the bottom of the window to perform the following operations:

- Refresh
  Click this button to update the display of the Network and Router information from the Administration Database.

- Apply
  is enabled when all the required fields in the Details panel have been filled. Click this button to add the provisioning information to the Administration Database.

- **Cancel**
  Cancel what you have entered in the Details panel at any time BEFORE you click the Apply button.

Preside MDM

IP VPN Service Configuration

R15.1

Publication: 241-6001-616
Document status: Standard
Document version: 15.1RSUP
Document date: August 2004
Printed in Canada