Oracle® Communications IP Service Activator

VPN User's Guide

Release 7.2

E47719-01

October 2013

ORACLE®

Oracle Communications IP Service Activator VPN User's Guide, Release 7.2

E47719-01

Contents

2 Setting Up Layer 3 Multicast Services

3 Setting Up Layer 2 Martini VPNs

4 Setting Up Dedicated Internet Access Services

5 VLAN Configuration in Metro Ethernets

Preface

This guide explains how to configure RFC4364 MPLS-based VPNs, Layer 3 Multicast and Dedicated Internet Access services, Layer 2 Martini VPNs, Metro Ethernet VLANs, IPsec, and Transparent LAN Services. It explains how to create interfaces and subinterfaces using configuration policies.

Audience

This guide is intended for operations managers, administrators, and activation technicians who are responsible for setting up VPN services using Oracle Communications IP Service Activator.

Related Documents

For more information, see the following documents in the IP Service Activator documentation set:

- See *IP Service Activator Installation Guide* for instructions on installing and upgrading IP Service Activator components and modules.
- See *IP Service Activator Administrator's Guide* for information and procedures related the duties a system administrator performs in monitoring and managing IP Service Activator.
- See *IP Service Activator Network and SLA Monitoring Guide* for information about applying and generating measurement data, and allocating quality of service (QoS) based on service level agreements.
- See *IP Service Activator QoS User's Guide* for information about configuring QoS and access control policies with IP Service Activator.
- See the MPLS LSP module in IP Service Activator online Help for information on configuring Multiprotocol Label Switching (MPLS) Label Switched Paths (LSPs).

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or

visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

1

Setting Up MPLS VPNs

This chapter explains how to set up RFC4364bis multiprotocol label switching (MPLS) virtual private networks (VPNs) within your Cisco or Juniper M-series-based networks.

About MPLS VPNs

An IP virtual private network (VPN) is a means of creating a private network over a shared IP infrastructure. A VPN enables a secure, private connection between a number of geographically remote customer sites. VPNs can be used to implement corporate intranets, linking remote offices or mobile workers, and extranets, extending the services to customers, suppliers or other communities of interest.

Oracle Communications IP Service Activator supports VPNs based on RFC4364bis, a widely supported IETF standard. This is an architecture based on using MPLS to forward packets over the backbone and using BGP (Border Gateway Protocol) to distribute routes.

MPLS VPNs are based on Layer 3 connectionless technology. The primary advantage of this is that MPLS VPNs are much more scalable than other IP VPN technologies, as there is no need to create a full mesh of tunnels or permanent VCs between all sites in the VPN. Deploying and managing an MPLS VPN is therefore more straightforward than the VC-based or IP tunneling options.

Security and privacy within an MPLS VPN is achieved by limiting the distribution of routing information to all members of the VPN. Routes to VPN sites are only advertised to members of the same VPN, and are not shared with core devices or devices outside the VPN.

IP Service Activator allows you to set up VPNs quickly and easily by defining appropriate customer sites and specifying how they are linked together into VPNs. The relevant routers throughout the network are then configured automatically. VPN membership can be updated by adding and deleting customer sites when required.

Note: Minimal manual configuration of routers is initially required.

IP Service Activator supports MPLS VPNs implemented within Cisco, Juniper M-series, Brocade, Huawei AR, or Huawei NE networks. Oracle strongly recommends that you read the relevant device driver or device cartridge guide before setting up an MPLS VPN. Support for additional devices can be added by creating a new cartridge using the IP Service Activator Software Development Kit (SDK).

Note: Not all services are supported by all equipment vendors. See *IP Service Activator Installation Guide* and the appropriate Cartridge or Device Driver guides to confirm support for the services you wish to implement.

Planning MPLS VPNs

Consider the following points before setting up VPNs:

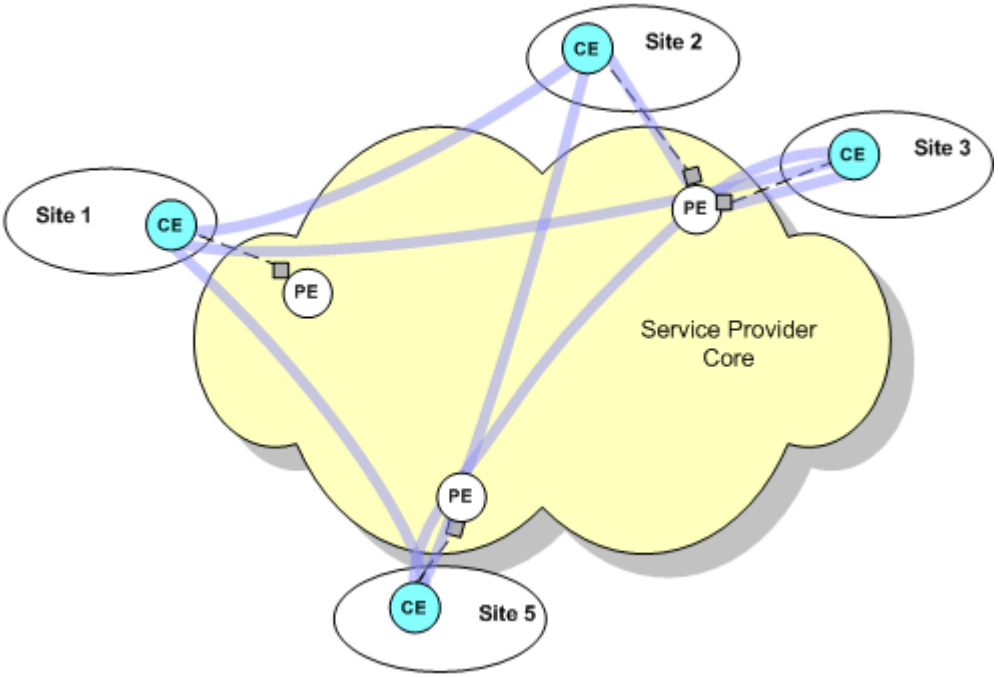
- VPN Topology
- Routing Protocols

VPN Topology

There are two types of VPN topology: fully-meshed, and hub and spoke.

In a fully-meshed VPN, each customer site can communicate with all other sites. Figure 1–1 illustrates the way in which sites communicate in a fully-meshed VPN topology.

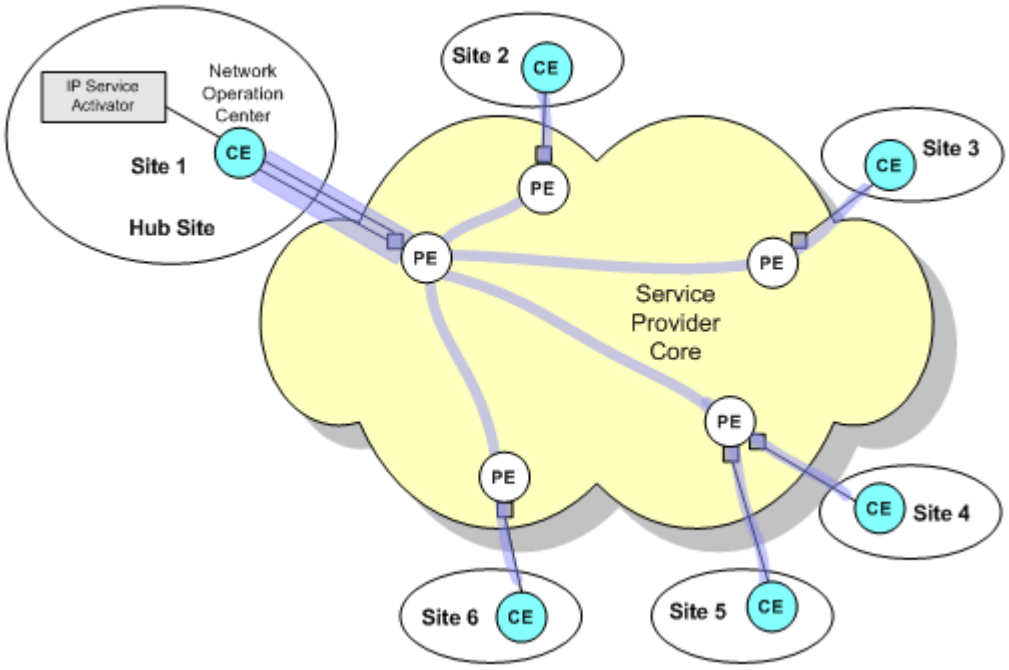
Figure 1–1 Site Communication in a Fully-meshed VPN Topology



A site can participate in any number of fully-meshed VPNs.

In a hub and spoke VPN, one or more sites act as a hub or management interface. Figure 1–2 shows the way in which sites use a hub to communicate in a hub and spoke VPN topology. Sites 2, 3, 4, 5, and 6 are only aware of Site 1, while Site 1 can communicate with all other sites.

Figure 1–2 Site Communication in a Hub and Spoke VPN Topology



Each site must be defined as a hub or a spoke. A site may be a member of several hub and spoke VPNs and act as a hub in one VPN and a spoke in another. There may be more than one hub site in a hub and spoke VPN or, alternatively, all sites may be defined as spokes.

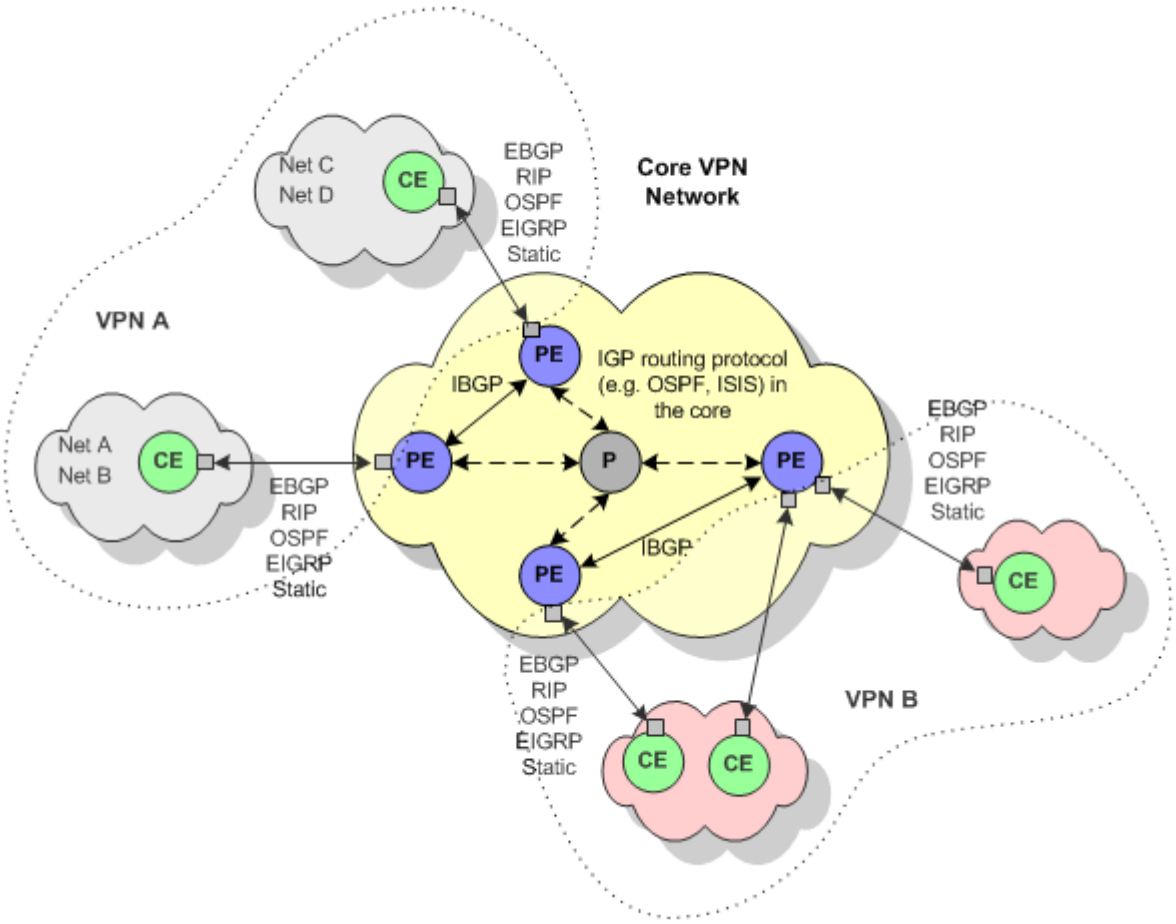
A management VPN is a special type of hub and spoke VPN that provides connectivity to CE devices and reduces the risk of connectivity loss. Create a management VPN if you intend to apply QoS or Service Assurance Agent (SAA) to a hub and spoke or fully-meshed VPN. For more information, see "Management VPNs".

Note: You can modify either fully-meshed or hub and spoke VPN topology by manipulating VPN route targets or using route policies and route maps.

Routing Protocols

The various routers within the VPN need to communicate using a routing protocol. Figure 1–3 illustrates routing in an MPLS VPN.

Figure 1–3 Routing in an MPLS VPN



A BGP autonomous system is a collection of networks. Each autonomous system is identified by an autonomous system number (ASN), which is required when running BGP. In order to configure BGP, you need to assign an ASN to each customer site network, in addition to the service provider core network. eBGP is a variant of BGP that connects the Provider Edge (PE) router to a Customer Edge (CE) router where both the provider and customer networks are running iBGP.

Each PE router also needs to communicate with its external neighbors (the CE routers to which it is connected).

In addition to static routing, IP Service Activator supports the following routing protocols:

- External BGP (eBGP)
- RIP (Routing Information Protocol)
- OSPF (Open Shortest Path First)
- EIGRP
- EBGP & OSPF
- EBGP & RIP
- EBGP & EIGRP
- None

For information on device support for routing protocols within IP Service Activator, see the appropriate Device Driver or Cartridge guide.

IP Service Activator can configure static routes between the PE and CE router. Static routes may be used in combination with any routing protocol. For multi-homed sites, you can configure a static route per PE interface. For eBGP and static routing, you must set up appropriate routing parameters so that the PE router can be configured appropriately.

You can specify a metric to associate with routes as they are distributed from the PE-CE routing protocol into other IGPs and BGP and vice versa. For more information, see "Specifying Metrics for Route Redistribution".

Note: IP Service Activator supports multi-AS BGP VPN configurations. Refer to the Cartridge guides for your device types for details

Options for Handling VRF Tables

A VPN must be secure and maintain data separation; it must prevent communication between sites that are not in the same VPN. One way to do this is to ensure that VPNs have their own routing tables in the PE router, so a customer site that belongs to a VPN can access only the set of routes contained in that routing table.

Each PE router maintains a number of separate forwarding tables known as VRF (VPN Routing and Forwarding instance) tables, and each site (that is, each PE interface or sub-interface connected to a CE device) must be mapped to one of those VRF tables.

A VRF table does not necessarily correspond to a particular VPN. Its purpose is to hold the routes that are available to a particular site connected to a PE device. If a site is in multiple VPNs, the VRF table associated with that site contains routes within all the VPNs of which it is a member.

Using VPN-wide or Site-Specific VRF Details

By default, IP Service Activator automatically generates a site-specific VRF table name and Route Distinguisher (RD) for each site that participates in a VPN. In a typical MPLS VPN setup, the RD uniquely identifies the site.

However, you can override the IP Service Activator default by specifying at the VPN level that the same VRF table name and RD number is applied to all sites that participate in the VPN. You can choose whether to use IP Service Activator-generated values or specify your own VRF table name and/or RD number. Sites that participate in the VPN must be set to inherit VRF\RD details from the VPN.

A site may be set to inherit VRF/RD details and be a member of more than one VPN that specifies VPN-wide VRF/RD details. In this situation, IP Service Activator's default behavior is to generate VRF/RD details for the site to avoid any conflict. However, it is possible to specify, in cases where a site inherits VPN-wide VRF/RD details from multiple VPNs, user-defined details specified at site level are used instead.

IP Service Activator allows you the following options for defining the VRF table name and RD. You can:

- Specify that the same VRF table name and/or RD is used by all sites within a VPN.

You can choose whether to accept the identifiers generated by IP Service Activator or create user-defined identifiers.

- Specify that each site has a manually-defined VRF table name and/or RD.

  Using a single RD number for all sites in a VPN is suitable only where a site belongs to one intranet VPN. If the site may become a member of an extranet VPN in the future, this method is not recommended.

- Specify that, if a site is member of only one VPN, its VRF table name and RD are derived from the VPN and, if a site is part of more than one VPN, its VRF table name and RD are manually defined at the site level.

For more information, see "Setting Advanced VRF Table Options" and "Using an RD Number per VPN or per Site".

VRF Re-use and Reduction

VRF reduction helps minimize device resource usage. From a logical point of view, each VRF table maps onto an interface in a site (except with interface-less VRFs). However, having a VRF table for each PE interface in a site will create scalability problems on the router. Therefore, if multiple VRF tables contain exactly the same routing information (for example, if one site connects to two interfaces, or there are two sites that are members of the same VPN) and the routing protocol behaviors are identical or compatible between them, IP Service Activator normally reduces them to just one VRF table, in order to minimize resource usage. This is known as VRF reduction.

IP Service Activator uses different methods to perform this process depending on whether you are using system-generated or manually defined VRF table names.

Where system-defined VRF table names are used, VRF reduction is based on the site's RD number. Sites with lower RD numbers takes precedence over sites with higher RD numbers. Note that no reduction occurs under the Network Processor for VRFs on sites with different RD numbers.

Where user-defined VRF table names are used, IP Service Activator performs VRF reduction based on table names. If you are using user-defined VRF table names, VRFs can only be reduced into other VRFs that have matching table names.

When a new VRF table creation request is sent to the device driver, the driver first attempts to reduce the VRF table into an existing IP Service Activator provisioned VRF. If this is not possible, a new VRF is provisioned. In case of multiple concurrent VRF table creation requests, the driver evaluates the request in the order of increasing site RD numbers (for system-defined VRF table names) or in the ASCII sort order of the VRF table names (for user-defined VRF table names).

VRF Parameters: Force Install and Shareable

You can override VRF re-use by specifying that particular interfaces are always to have their own VRF table. You can also specify that other VRF tables are allowed to be merged with this VRF table by selecting Shareable VRF.

If a new VRF has the Force Install attribute set, it ensures that a VRF table is will be created for the selected site, but it will not be reduced into other VRFs. As a result, in some circumstances, identical VRF tables may be configured on the device. This attribute is set on the VRF property page of the Site dialog box, by selecting Force Install from the VRF table re-use panel. The default is for Force Install not to be set.

Using Force Install also ensures that an Interface/SiteAddress is the first one in its VRF.

Once Force Install is selected, you can optionally select Shareable.

If the Shareable attribute is turned on, then other VRF tables are allowed to be merged with the VRF. The default is for Shareable not to be set.

The Shareable attribute is only selectable when Force Install is also set for the site.

If VPN attributes or routing protocol attributes do not match or are incompatible no reduction is performed.

VRF Master Sites

When a VRF is initially created, the site which triggered the creation of the new VRF is known as the VRF master site and the VRF is known as the VRF master. (This is a conceptual designation and is not reflected in the IP Service Activator client in any way.) If other VRF tables are reduced into this VRF, there is a dependency on the VRF master.

If the VRF master site is taken out of the VPN, the VRF master is de-provisioned. All remaining interfaces are reduced into a newly created VRF master. Accordingly, one of the interfaces' sites in the VPN will become the new VRF master site for the new VRF master.

If the VRF master site is modified such that its VRF (the VRF master) is no longer compatible with the other VRF tables which are reduced into it, the interfaces of the other sites are removed from the VRF master before the VRF master is modified to reflect the new VRF master site properties. The removed interfaces are reduced into a newly created VRF. Again, one of these interfaces' sites will become the new VRF master site for this new VRF master in accordance with the logic explained above.

During the re-provisioning which occurs as a result of either of the above scenarios, the interfaces moved to the new VRF temporarily lose connectivity and trigger routing re-convergence.

During VRF reduction, the Network Processor and Cisco Device Driver send alias commands to track which sites use the newly reduced VRF on the router. This information can help determine which site is the VRF master site, so you can ensure that a VRF master is not removed when there are still sites reduced into it.

Configuration Preservation

Normally, when parameters supplied to a particular site match with another site in the same VPN, VRF reduction occurs into the VRF master. The VRF master is retained and the other VRFs which were reduced are removed since they are redundant.

The device driver and Network Processor will try to preserve configuration for already provisioned VRFs on the device in cases where performing VRF reduction would potentially cause a network outage.

When a valid parameter is changed on a merged VRF, the VRFs are unmerged. After that, the VRF will not reduce again, in accordance with the configuration preservation concepts described above. (If there is a need to merge VRF sites again, you can unlink the sites, and link them back.) There are some exceptions to this:

- With the device driver, changing the VRF import/export map in multiple sites to the same name
- On the Network Processor, changing a generated RD to a user-specified RD, and vice-versa

In both these cases non-reduced VRFs are reduced to a common VRF.

When VRF Reduction Does Not Occur

There are a number of parameters that don't affect reduction behavior - particularly, when route redistribution protocols and static routes match between VRFs.

The following do not affect VRF reduction behavior

- RIP Properties, including Ignore Routes, Passive Interface
- OSPF Properties, including Distribute-in Filter, Cost
- EBGP: Neighbor data
- Static routes

In general, commands that are not part of the actual VRF configuration commands on the device do not change VRF reduction behavior.

VRF Reduction in Orthogonal Combinations

In addition to configuration parameters, an orthogonal combination of parameters does not stop VRFs from reducing.

Consider a scenario in which you have two sites with different routing protocols applied, EIGRP on one and OSPF on the other. These sites will reduce to single VRF, provided all the other parameters are equal.

However if two sites have the same routing protocols, but have different routing parameter values set, they will not reduce. An example of this is two sites both configured to use OSPF, but with different SpfThrottling parameter values.

VRF Reduction in Hub and Spoke VPNs

In IP Service Activator, the default VPN topology is fully meshed. This can be changed as required.

> **Note:** If there is no reduction for VRFs in a mesh topology VPN, there will be no reduction for VRFs in a hub and spoke topology VPN.

The VRF reduction behavior in hub and spoke topology is identical for the Cisco Cartridge and Cisco device driver. However, there is a difference in behavior when the topology is changed.

Table 1–1 shows VRF reduction behaviors for both the Cisco Cartridge and the Cisco device driver for source and target topologies. The target columns shows the changed behavior of the Cisco cartridge and the Cisco device driver when the topology changes to the target topology from the source topology. The table shows that the behavior between Cisco Cartridge and Cisco device driver changes when topology is changed from hub and spoke to Mesh.

Table 1–1 VRF Reduction Behaviors for Cisco Cartridge and Cisco Device Driver

Source Topology	Source Topology Cisco Cartridge Behavior	Source Topology Cisco Device Driver Behavior	Target Topology	Target Topolgy Cisco Cartridge Behavior	Target Topology Cisco Device Driver Behavior
Mesh	Reduction	Reduction	Hub and spoke	No Reduction	No Reduction
One hub, multiple spokes	No Reduction	No Reduction	Mesh	No Reduction	No Reduction
Mesh	N/A	N/A	Multiple hubs, multipls spokes	Reduction among hub sites, separate VRF for each spoke	Reduction among hub sites, separate VRF for each spoke
Multiple hubs, multiple spokes	N/A	N/A	Mesh	Reduction among hub sites, separate VRF for each spoke	Reduction

Interface-less VRFs and Sites

IP Service Activator supports the indirect creation of interface-less VRFs and therefore interface-less Sites. An interface-less VPN site models a VRF on a router where no interface points to the VRF.

For complete details about interface-less VRFs and sites, see the IP Service Activator online Help.

Service Application Points

When an interface-less Site and VRF are created, an object called a Service Application Point is modelled in the background and linked to the Site. The Service Application Point object behaves similarly to an interface (and has a role of Access for purposes of supporting the interface-less Site and VRF) but it is not accessible or modifiable through the GUI. The PE device is displayed in the Access Points folder for the site in order to represent the Service Access Point.

Service Application Point objects are exposed in the EOM and are accessible through the OSS Integration Manager interface. See *IP Service Activator OSS Integration Manager Guide* for details.

Creating an Interface-less Site and VRF

To create an interface-less VRF, first create a VPN Site. Then, drag the entire PE device into the site as you normally would an interface. This creates the Service Application Point and causes the PE symbol to be displayed in the Access Points folder of the Site to represent it. (See below).

Once created, the Site can participate in VPNs in a similar fashion to site with an attached interface.

Site Properties: VRF Router-ID Attribute

The **router-id** attribute is available on the Site dialog box, Site VRF property page. This attribute is used when OSPF routing is enabled on a device, becoming the configured OSPF router ID. The **router-id** attribute can be configured on Cisco, Alcatel, and Brocade devices only.

The router-id can be set on a VRF regardless of the routing protocol chosen for the site. However if OSPF or EBGP is chosen as routing protocol, a router-id must be set or an error is returned. This error indicates that the SiteAddress requires a router-id.

When a VPN is committed, the device driver attempts to reduce the number of VRFs. During this process IP Service Activator ignores all the router-id properties except for one: the selection of the router-id as discussed below. Once the VRF has been reduced, it is created on the device. Before setting the router-id parameter in the VRF, the driver creates a loopback interface and binds it to the VRF. The appropriate IP address will also be set on this newly created loopback interface.

If a VRF is initially created for one interface, this interface/SiteAddress will remain designated as 'the one containing the router-id' for the entire life of that VRF regardless of the number of interfaces that are subsequently added to it. The router-id can be added, if desired, to the first interface bound (and committed) to a VRF. Using Force Install also ensures that an Interface/SiteAddress is the first one in its VRF. See "VRF Parameters: Force Install and Shareable".

Unless loopback interfaces are filtered out during the discovery process, subsequent device re-discoveries may find the newly created loopback interfaces and display them in the client. Do not attempt to use them.

Some operations such as setting a specific VRF name, route distinguisher, or DHCP Helper to a SiteAddress may force a VRF 'split'. In this case, the router-id requirements may no longer be met for the target configuration. An error is returned indicating which SiteAddresses require an additional router-id.

Note: If you unmanage a device, then make a change to it (such as a VRF parameter) and then commit these two actions in the same transaction, the change is saved in the IP Service Activator database, but is not propagated to the device.

If you remanage the device in a subsequent transaction, there is loss of synchronization between the device and the IP Service Activator database. If this occurs, repeat the change in a new transaction.

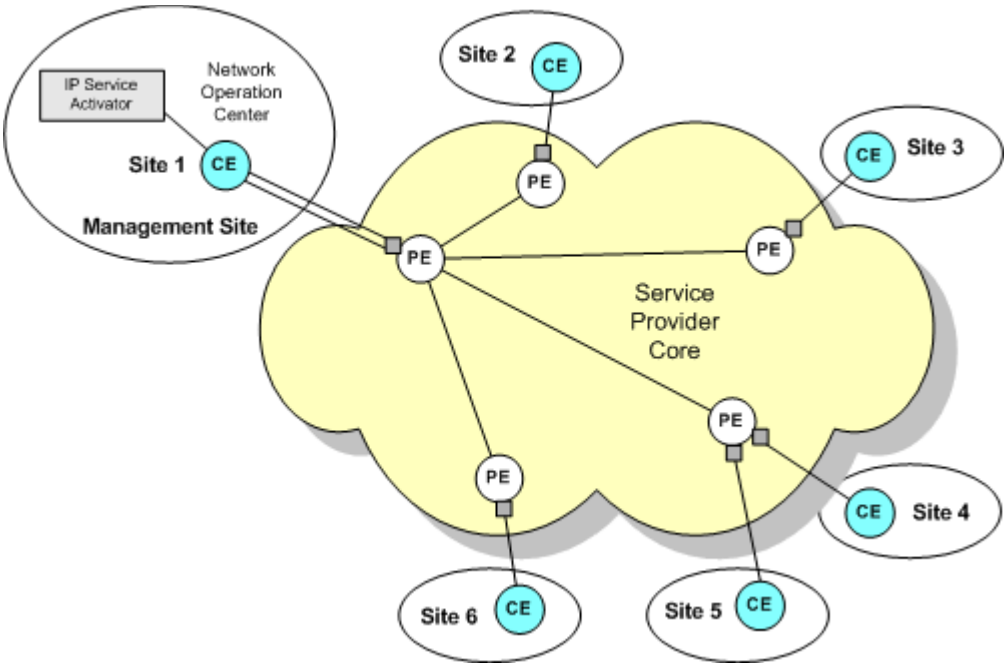
Do not unmanage a device and make a change to the device in the same transaction.

Loss of synchronization also occurs if you make manual changes to a device which has been unmanaged, and is later remanaged. If this occurs, manually remove the incorrect configuration from the device.

Management VPNs

If you require visibility of the customer's CE devices, for example, to apply QoS or measurement at the CE devices, you should set up a management VPN. The management VPN provides connectivity to CE or shadow devices and avoids potential loss of connectivity. Figure 1–4 illustrates a management VPN using hub and spoke topology.

Figure 1–4 Management VPN Using Hub and Spoke Topology



In IP Service Activator, a VPN is always associated with a customer object. One technique is to create a Customer named 'Management' and create the management VPN beneath this. Then create the 'real' Customer which maps to the real-world customer, and create a hub and spoke or fully-meshed VPN.

For a summary of the steps involved in setting up a management VPN, see "Setting Up Management and Customer VPNs".

Applying Services to a VPN

IP Service Activator's policy management features allow you to apply Quality of Service (QoS) throughout the VPN. Network traffic can be divided into separate classes of service and allocated quality of service characteristics according to service level agreements with the customer. For more information see *IP Service Activator Network and SLA Monitoring Guide*.

> **Note:** When applying QoS to a VPN, policy that has been applied to a customer is inherited to a site, unless the site is a member of a VPN to which a policy element of the same type has been applied. In this case, the policy applied to the VPN overrides that applied to the customer.

Measurement can also be applied to the VPN using Service Assurance Agent (SAA). SAA is a Cisco technology that enables you to apply measurement to point-to-point connections within an MPLS VPN or a measurement-only VPN. In a measurement-only VPN, devices are grouped solely for the purpose of applying measurement. For more information see *IP Service Activator Network and SLA Monitoring Guide*.

Setting Up an MPLS VPN

The following steps are involved in setting up a VPN within IP Service Activator:

- Set up domain-specific parameters. See "Setting Up Domain Parameters".
- Discover the network and assign roles. See "Discovering the Network and Assigning Roles".
- Set up the customer sites that are to be connected by a VPN, including information about their routing parameters. See "Setting Up Customers" and "Setting Up Sites".
- Associate each site with the appropriate access interface on a PE (gateway) router. See "Setting Up PE-CE Routing Parameters".
  - If you need to create interfaces and/or sub-interfaces to use as the access point on the PE router, use the appropriate interface creation policy. See "Registering Interface Policies and Creating Interfaces".
  - If you are creating interfaces off controllers, set up your discovery to discover controllers. For more information, see the discussion of customizing discovery using **AutoDiscovery.cfg** in *IP Service Activator Administrator's Guide*.
- Set up a VPN object and link the customer sites to it by dragging and dropping. See "Setting Up the VPN".

Note: Minimal manual configuration of routers is initially required. See "Manual Preconfiguration".

Before Setting Up an MPLS VPN

This section explains the tasks to perform before setting up a VPN. The tasks are:

- Manual Preconfiguration
- Setting Up Domain Parameters
- Discovering the Network and Assigning Roles
- Assigning Devices to Proxy Agents
- Setting Devices to Managed

Manual Preconfiguration

Before setting up VPNs, some manual configuration of routers will likely be required. You must have your MPLS core set up to support VPNs. Please refer to the vendor documentation for details.

PE Routers and P Routers

You need to have a functional MPLS network in order to configure MPLS VPNs.

On all PE (gateway) and P (core) routers in the core network, you need to ensure that MPLS is enabled on core interfaces. An Interior Gateway Protocol (IGP) must be implemented in order to distribute IP routes.

Ensure also that all IP addresses are correctly assigned. It is a best practice to have a loopback interface set up.

The loopback interface specified at the domain level is used in the VPN context in that domain unless it is overridden at a lower level, that is, on the Site dialog box. If you

have configured iBGP peering (which should be done manually, not using IP Service Activator), you should use the same loopback interface on all devices which will be included in the VPN.

The loopback interface should be reachable.

On Cisco devices, ensure that CEF (Cisco Express Forwarding) or dCEF (Distributed CEF) is configured, as it is a prerequisite for MPLS.

On Juniper M-series devices, you must configure LSPs between the loopback addresses of all PE and P devices.

User-defined VRF tables, export maps, prefix filters and route maps

You can manually preconfigure PE routers with your own data to allow greater flexibility or special operational requirements to be implemented for your MPLS VPNs.

VRF tables can be manually configured to invoke particular VPN behavior and other special requirements.

> **Note:** User-defined VRF tables are not supported on Juniper M-series devices that are managed by the Juniper M-series Device Driver.

Export maps can be manually configured with the prefixes of VRF table routes which you want exported to other PE routers. A VRF table route is only exported to other PE routers if its prefix matches one of those specified in the export map. The exported routes are tagged with a route target specified by the export map. This ensures that routes are only advertised to sites that need to receive them.

You can also manually configure route maps, or policy statements on Juniper M-series routers, to filter the routes that are redistributed between the protocols used for PE-CE connectivity within the VPN.

Route maps can also be configured through the use of the vrfRoutePolicy configuration policy and referenced in the site configuration in the same way you would reference a manually configured route map.

For details about the vrfRoutePolicy configuration policy, refer to IP Service Activator online Help.

Prefix filters can be manually configured with the prefixes of eBGP routes which you can specify are to be either accepted or denied by a VRF table. You can associate a prefix filter with incoming and/or outgoing routes.

CE Routers

In an IP Service Activator installation, CE routers can either be unmanaged, or managed by IP Service Activator with some restrictions.

When CE routers are managed, IP Service Activator can handle modelling and provisioning QoS. However, other than static routing, aspects of the configuration relating to VPNs must be handled manually, (other than some basic provisioning of static routes).

Ensure that the appropriate routing protocol or static routing is configured in order to advertise reachability information between the CE and the PE.

IP Service Activator can be used to apply global static routes to the CE in order to set up routes between the PE and CE by using the staticRoutes configuration policy. Refer to the "Configuration Policy - staticRoutes" Online Help topic for details.

If you are using a routing protocol (such as eBGP or EIGRP) for communication between the PE and CE rather than 'hard-wired' static routes, there are a number of approaches that can be used to configure the CE. You can set up the routing protocol on the CE manually, use a Configuration Template Manager template to do it, or use the IP Service Activator SDK to create a configuration policy to do the needed configuration.

You should also set up a loopback interface on each CE router and configure it to carry IP traffic.

Setting Up Domain Parameters

Before setting up the VPN, you should ensure the appropriate parameters are set up correctly on the tabs in the Domain dialog box (these may have been set up when the domain was created).

These parameters define:

- The number of alternative routes held by each PE to peer PE devices
- Whether BGP routes use the standard or extended community attribute or both
- Whether secure TCP connections are configured between iBGP peers using MD5
- Which interface is used as the loopback interface

> **Note:** The Network Processor does not support iBGP peering.

For complete information about setting up and configuring domains, refer to *IP Service Activator User's Guide*.

For complete dialog box and property page descriptions, see IP Service Activator online Help.

To check the domain parameters:

1. Display the Global Setup window.
2. Select the **Domain** tab, right-click the relevant domain and select **Properties** from the context menu.

   The Domain dialog box for the selected domain is displayed.
3. On the Domain property page, check the following parameters:
   - The domain Type must be **MPLS VPN**.
   - The Public PE to CE Addresses check box specifies whether public or private addresses are used on PE routers. If selected, it indicates that the PE interface connected to a CE router uses a public address. If deselected, the PE interface is assumed to use a private address.

> **Note:** The **Manual config** field enables you to specify how IP Service Activator handles manual preconfiguration on the device. This is valid for Device Driver only.
>
> IP Service Activator never deletes manually preconfigured VRF tables even if you select the **Delete** or **Warn and delete** options. If you select **Fail and don't delete**, no configuration is installed.
>
> The value set in the **Manual config** field on the Domain and Device property pages, including **Warn and Delete**, only applies to devices managed through the Cisco Device Driver. For example, the Juniper M-series Device Driver cannot be set up to monitor for or warn when changes to device configuration are made by other users. However, IP Service Activator can co-exist with manually applied configuration.

4. Select the VPN BGP property page.
5. Specify values including **Configure iBGP Peering**, **CE Site AS Override**, **Allow AS in**, **Maximum Paths**, **Send Communities**, **PE-PE MD5 Authentication**, and **Loopback ID**.

   If you want to use iBGP peering, it must be configured manually on your devices and not through IP Service Activator. Do not check **Configure iBGP Peering**. With this check box unselected, IP Service Activator leaves all iBGP configuration untouched. This means that whatever is installed will remain on the device.

> **Note:** On Juniper M-series devices, the loopback ID must always be specified as 0 through the client.

Specifying a VRF Route Limit

You can specify the maximum number of routes that can be added to the VRF table maintained by each PE peer within the domain. You can also specify a threshold value at which a warning message is generated in the router log either when the limit is reached or when a percentage of the limit is reached. By default, no VRF route limit is specified.

You can also override the limit defined at the domain and specify a different setting for a particular site. For more information, see "Setting Advanced VRF Table Options".

To specify a VRF route limit:

1. Display the Domain dialog box and select the **VPN MPLS** property page.
2. Select the **VRF Route Limit** check box.
3. In the **Max Route** field, enter the maximum number of routes that can be added to a PE router's VRF table.
4. Select either **Warn only** or **Warn at n%** from the Notification combo box.

> **Note:** Enter the string **Warn only at n%** into the text field to the left of the Notification combo box to manually to push the warning-only keyword. The string **Warn only at** is case sensitive.

Setting Up the Provider Core ASN for the Domain

To enable BGP communication throughout the VPN you must set the ASN for the domain.

To set the ASN for the domain:

1. Display the Domain dialog box and select the **ASN** property page.
2. Specify a value in the **Internal BGP ASN** field.

Discovering the Network and Assigning Roles

At this point you can run the discovery process to find all the P and PE routers in the network and include their details in IP Service Activator's database.

For information about running the discovery process, see the chapter about discovering and setting up the network in the *IP Service Activator User's Guide*.

Note the following:

- In an MPLS domain, the core provider network is assumed to use public addresses, and a hop count can be specified to discover further connected devices. All CE routers are assumed to use private addresses and an IP address or DNS name must be specified in order to discover them.
- All devices within the network must be correctly assigned system-defined roles, that is, PE routers must be classified as gateway devices, P routers classified as core devices and CE routers, if visible, as access devices. Assign roles manually for each device. For more information, see *IP Service Activator User's Guide*.

  Note: The system-defined **Shadow** role may be assigned to shadow routers associated with PE devices for the purpose of generating SAA measurement data. For more information, see *IP Service Activator Network and SLA Monitoring Guide*.

- All interfaces within the network must be correctly assigned system-defined roles:
  - On CE (access) devices, the interface connected to the PE device must be classified as an access interface. Interfaces connected to local segments must be classified as local interfaces.
  - On PE (gateway) devices, the interface connected to the CE device must be classified as an access interface. Interfaces connected to other PE devices or P (core) devices must be classified as core interfaces.
  - All interfaces on P (core) devices should be classified as core interfaces.

  You need to assign a role manually for each interface. For information about defining and applying roles, see the *IP Service Activator User's Guide*.

  Note: If the PE interfaces connected to CE devices have private addresses, that is, if the **Public PE to CE Addresses** check box on the Domain dialog box is deselected, connectivity cannot be determined. Therefore, CE devices and access interfaces on PE devices will not automatically be connected to segments and interfaces will not automatically be assigned roles. The connections between the PE and CE can be applied manually by dragging one interface on to another on the map or set manually from the CE.

Assigning Devices to Proxy Agents

All devices that are to be managed by IP Service Activator must be assigned to a proxy agent. This is generally performed automatically during device discovery, but if devices are not assigned to the correct proxy agents you must assign them manually. For information on assigning devices to proxy agents, see *IP Service Activator User's Guide*.

Setting Devices to Managed

All devices to be configured by IP Service Activator must have their status set to **Managed**. When devices are first discovered, their status is **Unmanaged**.

To set all devices to Managed:

1. Select **Manage All Devices** from the network or network map's context menu.

To set an individual device to Managed:

1. Select **Manage Device** from the device's context menu.

The device's color changes to reflect its new status. A managed device is represented by a green icon, an unmanaged device is represented by a blue icon.

Setting Up Customers

You must create a customer before you can create the sites and VPNs that feature in a service.

To set up a customer:

1. On the Service tab, right-click the **Customers** folder and select **Add Customer** from the context menu.

   The Customer dialog box opens.

2. Enter values including **Customer name**, **Remarks**, and **Reference**.
3. Click **OK**.
4. Commit the transaction.

Setting Up Sites

You must set up a site for each member of a VPN. Sites are created on a per-customer basis. You cannot create a site that is customer-independent. You can associate a site with more than one customer. Site are configured using the Site dialog box, which is accessible as described below when the Service tab is selected.

To set up a site:

1. On the Service tab, under the Customers folder, right-click the **Sites** folder and select **Add VPN Site** from the context menu.

   The site object appears on the Service tab and the Site dialog box opens.

2. On the Site property page, specify an identifying **Name** for the site, and any additional comments. You can set up account and contact information if required, but this is optional.
3. Click **OK**.

Note: Dragging a PE interface into a site adds the IP address of that interface to the Addressing property page and avoids the need to enter the address manually. See "Setting Up Private and Public Addresses for PE Interfaces".

Associating a Physical Component with a Site

Each site within a VPN must be defined by a physical network component with the exception of interface-less sites (for more about interface-less sites, see "Interface-less VRFs and Sites"). Typically a specific interface or device must be attached to the site in order to enable full routing information to be distributed throughout the VPN.

Linking a PE Access Interface

You need to link the access interface of the appropriate gateway (PE) router to the site.

Once you link an interface with a site and define its routing details, IP Service Activator maintains that information even if you subsequently remove that interface from the site. This means that you can re-use routing details if you change the interface that is associated with a site.

For a multi-homed site, you can link one or many PE interfaces to the site.

To link a PE access interface:

1. Drag and drop the appropriate access interface on the gateway device onto the site.
2. If there are existing unused interface address details associated with the site, the Site Addresses dialog box opens:
   - Create a new Site Address: Create new public/private IP address details for the interface being linked.
   - Attach to an existing Site Address: Use existing address details; select an address from the list.

Linking a CE Router

If IP Service Activator has visibility of site CE or virtual CE routers, you should also link the CE or virtual CE device directly to the site. This is only required if the service provider is offering a fully-managed VPN service and has complete visibility of the customer's devices.

When a configuration object (like QoS, configuration policies, and so on) is applied on the customer site or VPN, the configuration object is applied on the CE or virtual CE based on role-matching rules.

For a multi-homed site, you can drag multiple corresponding CE or virtual CEs into the site.

To link the CE device:

1. Drag and drop the access device on to the site.

Setting Up PE-CE Routing Parameters

Support for particular protocols is device dependent. Consult the relevant device driver guide for details of the protocols supported.

You must set up details of the routing protocol used between the PE router and the CE router. These can be either static or dynamic routing protocols. Different parameters are required for each. Static routing can be used in combination with other routing protocols. Static routes can be configured per PE interface for multi-homed sites.

For information on specifying the metrics to apply to routes as they are redistributed between protocols, see "Specifying Metrics for Route Redistribution".

You can also select a routing protocol type of 'None' to distribute routes to VPN peers without configuring PE to CE routing.

Note: Site of Origin (SOO) is configured automatically for sites that have more than one CE to PE connection where eBGP is used for PE-CE connectivity. For configuration details, see the appropriate device driver and cartridge guides.

For more information about setting up routing, see IP Service Activator online Help.

To select a PE-CE routing parameter:

1. Display the Site dialog box and select the **Connectivity** property page.
2. Specify the Routing Type. Select from **EBGP**, **RIP**, **OSPF**, **EIGRP**, **EBGP & OSPF**, **EBGP & RIP**, **EBGP & EIGRP** or **None**.
   - If **EBGP** is selected, you must supply additional routing parameters on the **EBGP** property page and, optionally, the **EBGP Advanced**, **Route Maps**, and **EBGP Dampening** property pages. See "Configuring eBGP Parameters".
   - If **RIP** is selected, additional parameters are available on the **RIP** property page. See "Setting Up RIP Properties for a Site".
   - If **OSPF** is selected, you may want to supply additional routing parameters. See "Setting Up OSPF Properties for a Site".
   - If **EIGRP** is selected, the **EIGRP** panel fields are available. See "Setting Up EIGRP Properties for a Site". You must specify redistribution of routes into BGP on the **Redistribution into BGP** property page and redistribution of routes into EIGRP on the **Redistribution into EIGRP** property page. Static Routing and its associated options are still supported as well, but options related to other routing protocols like BGP and OSPF are not.
   - If **EBGP & OSPF** is selected, both protocols are configured for the site. Static routing is still supported. Configure additional options for both protocols including route redistribution. See "Configuring eBGP Parameters" and "Setting Up OSPF Properties for a Site".
   - If **EBGP & RIP** is selected, both protocols are configured for the site. Static routing is still supported as well. Configure additional options for both protocols including route redistribution. See "Configuring eBGP Parameters" and "Setting Up RIP Properties for a Site".
   - If **EBGP & EIGRP** is selected, both protocols are configured on the interfaces in the site. See "Configuring eBGP Parameters" and "Setting Up EIGRP Properties for a Site". You must specify redistribution of routes into BGP on the **Redistribution into EBGP** property page, and redistribution of routes into EIGRP on the **Redistribution into EIGRP** property page.

- If **None** is selected, directly-connected VPN routes can be automatically redistributed to VPN members without path configuration by a routing protocol. This option should be used with option Redistribute connected.

  Select **None** if you wish to configure static routes between the PE and CE device instead of a routing protocol.

3. Specify values including **Static Routing**, **Redistribute Routes**, **Local Routes**, **Domain Tag**, and **Generated Site of Origin**.

For information on defining static routes, see "Configuring Static Routing Parameters".

You can also specify metrics for route redistribution between protocols. For information, see "Specifying Metrics for Route Redistribution".

Configuring eBGP Parameters

IP Service Activator provides control over eBGP configuration. You can:

- Specify the number of times the same ASN can occur in the AS_PATH attribute of a route prefix
- Specify the local preference for each interface in a multi-homed site
- Configure secure TCP connections between eBGP peers using authentication
- Define route dampening parameters
- Specify the number of alternative routes to the CE device that are maintained in the PE device's routing table

For more information about configuring eBGP parameters, see IP Service Activator online Help.

To specify eBGP parameters:

1. In the Site dialog box, select the **EBGP** property page.
2. Specify values including **Neighbour Address**, **AS Override**, **Remove private AS**, **Authentication**, and **EBGP Multihop**.
3. If **Set at site** is selected on the **VPN BGP** property page in the Domain dialog box, **AS Override** check box appears as selected.
4. In the Update Source drop-down, select default to use the PE Interface ID in the update-source interface. With the Network Processor, choose from **<Default>** and **<None>**. Selecting **<None>** avoids propagating the update source-interface EBGP command. Selecting **<Default>** (which is the default setting) propagates the update source-interface EBGP command using the PE interface itself as the source interface.
5. Under **Allow AS in**, select **Use domain default** check box to use the value specified on the **VPN BGP** property page in the Domain dialog box or select **Use** to specify a different value for the site. You can specify a value from 0 to 10 inclusive.
6. Under **Local ASN**, start configuring Local Autonomous System Numbers by selecting the **Enable local ASN** check box. In the **Local ASN** field, specify a numeric value to for the Autonomous Systems path attribute. Select **No Prepend** if required.
7. In the **Neighbour Description** field, enter a description of the neighbor or select default. Leaving this field empty avoids generating the neighbor description command.

8. If multiple PE interfaces or sub-interfaces are associated with a site, specify settings for each listed interface or sub-interface.

   Edit entries using the Set button.

9. If you want to define advanced eBGP parameters, select the **EBGP Advanced** property page.

10. Specify values for each listed PE interface or sub-interface including **Prefix Limit**, **Restart**, **Delay (minutes)**, **Prefix filters**, **Send Communities**, **Timers**, **EBGP Attributes**, **Route Filters**, **Neighbor connection**, **TCP Transport Session Options**, and **Advertisement Interval**.

11. On the **EBGP Route Maps** property page, specify eBGP Route-map parameters.

    IP Service Activator supports inbound and outbound external BGP route-maps applied on a per-neighbor basis for the site.

    Note: Use a naming scheme different from IP Service Activator's for external inbound and outbound route-maps. IP Service Activator will remove route-maps with the same names as those which it generates when **Use Autogenerated Route-map** in the **EBGP Route Maps** property page of the Site dialog box is enabled. This can also occur when the device is unmanaged and remanaged depending on the setting of the **Unmanage Action** attribute.

    Route-map names specified on this property page are not validated against the names of route-maps provisioned on the router. You must correctly specify names of the externally defined route-maps.

    EBGP Route maps can also be configured through the use of the **bgpRoutePolicy** configuration policy and referenced in the same way you would reference a manually configured route map.

    Applying the **bgpRoutePolicy** configuration policy (at the Site level, for example) creates the route map but does not apply it to the site. Once the configuration policy is applied, you must still refer to it in the inbound/outbound fields of the Site dialog box for it to have any effect.

    Refer to I*P Service Activator QoS User's Guide* for complete details on installing and applying configuration policies.

    For more information about configuration policies, see IP Service Activator online Help. The Configuration Policy - bgpRoutePolicy topic contains details on the fields available in this configuration policy.

12. Set the options for each PE interface listed in the Addressing and routing details listbox including I**nbound Route Map: Use External Route-Map**, **Use Generated Route-Map**, **Local Preference**, **Generated Site of Origin**, **Use Route Map Name**, and **Outbound Route Map: Use External Route-Map**.

13. If you wish to specify eBGP dampening parameters, select the **EBGP Dampening** property page.

    Route dampening is a mechanism that attempts to minimize instability by suppressing the advertisement of unstable routes. Penalties are applied when a route is withdrawn, re-advertised or changed. When a predefined penalty limit is reached, further advertisement of the route is suppressed. The penalty is reduced according to a defined 'half-life' setting, and once the penalty decreases below a limit, the route can be re-advertised.

EBGP dampening is supported on Cisco and Juniper M-series devices.

14. Select the EBGP Dampening check box and set options including **Decay Half-life**, **Reuse Threshold**, **Suppression Threshold**, and **Max Suppression Time**.

Configuring a Multi-AS Site VPN

IP Service Activator supports VPNs which bridge more than one Autonomous System. However, in order to create this type of VPN, the eBGP and iBGP peering sessions must be configured manually.

When the VPN is configured on a device which already contains an ASN, and IP Service Activator is told not to configure iBGP peering, the iBGP configuration already on the device is left unaltered, as is the ASN.

To create a site that bridges multiple Autonomous Systems:

1. Manually assign ASNs to the PE devices.
2. Manually configure iBGP peering on your network.
3. Manually configure eBGP peering between PEs in different AS clouds.
4. Perform the remainder of the VPN configuration in IP Service Activator as normal.

Configuring Static Routing Parameters

You can specify how IP Service Activator configures the next-hop parameter in a static route. Choices include:

- IP Address and Interface
- IP Address Only
- Interface Only
- Null Interface

By default, IP Service Activator configures static routes with the interface name, next hop IP address and metric. Other configuration choices include:

- Whether the next-hop-address is an address that is in the routing table and not the VRF table (Global check box)
- Whether the static route will not be removed even if the interface shuts down (Permanent check box)
- Whether a tag is to be associated with a static route, allowing it to be used by route map match statements controlling redistribution of routes (Use this tag field).

> **Note:** If you have manually configured static routes on the device, these routes are not removed by IP Service Activator provided the VRF table the routes are associated with is not controlled by IP Service Activator.

Controlling Redistribution of Static Routes

You can control whether or not static routes are redistributed into dynamic routing protocols.

To redistribute static routes:

1. On the **Connectivity** property page of the Site dialog box, select **Redistribute Routes**.

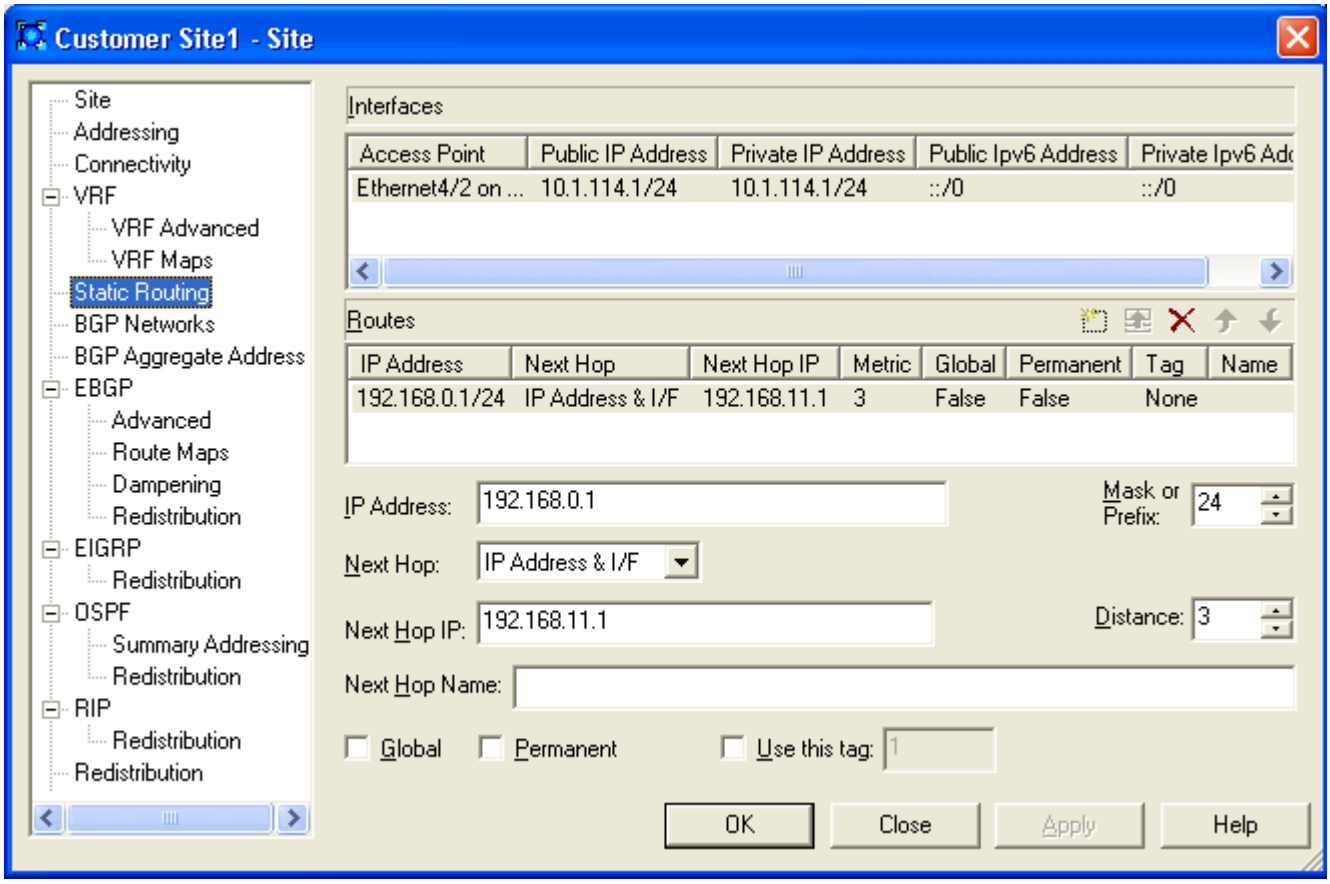
To have static routes remain local:

1. On the **Connectivity** property page of the Site dialog box, select **Local Routes**.

To specify static routing parameters:

1. In the Site dialog box, select the **Static Routing** property page. Figure 1–5 shows the **Static Routing** property page.

Figure 1–5 The Static Routing Property Page



Note: The fields on the **Static Routing** property page are disabled until the Static Routing check box on the **Connectivity** property page is selected.

2. Select a listed PE interface or sub-interface and specify values including **IP Address**, **Mask**, **Next Hop (Type)**, **Next Hop (IP Address)**, **Distance**, **Global**, **Permanent**, and **Use this tag**.

Setting Up Private and Public Addresses for PE Interfaces

When an interface is added to a VPN it leaves the public IP space and becomes part of a private IP space. Therefore for the PE access interface you need to set up public and private addresses. The public address applies when the interface is outside the VPN, and the private address applies when it is within the VPN.

To set up private and public addressing:

1. Display the Site dialog box and select the **Addressing** property page.

   Any PE interfaces or sub-interfaces that you have linked to the site are listed. If no PE interfaces or sub-interfaces have been linked to the site, no addresses appear.

2. Select the desired interface in the Addressing Details list, and supply values including **Public IP: IPv4 Address and Mask**, **IPv6 Address**, **Prefix Length**, **Private IPv4 Address: IP Address and Mask**, **Private IPv6 Address: IP Address** and **Prefix Length**, **Unnumbered**, and **Description**.

   For additional important notes on the Description field, see IP Service Activator online Help.

Configuring IP Unnumbered Private PE IP Addresses

IP Service Activator supports IP unnumbered Private PE addressing for certain serial point-to-point IP interfaces in VPN sites on Cisco devices. This allows you to enable IP on an interface and use it in a VPN without having to assign an explicit Private PE IP address and mask. Instead, the IP address of loopback address from the device is used.

To configure an interface for IP unnumbered addressing:

1. Display the Site dialog box and select the **Addressing** property page.
2. Select the **Unnumbered** check box for the Private PE IP address for the interface in the Site.
3. From the context menu, select the loopback interface that you want to provide an outgoing IP address for the interface.

> **Note:** When a site is created, by default, the Unnumbered addressing check box is unavailable. It becomes available when an interface is linked to the site. When the Unnumbered addressing check box is selected, you can then specify either a loopback interface, or other interface details.

See "Setting Up Private and Public Addresses for PE Interfaces" for details.

About Routing Protocols, VPNs, and IP Unnumbered

Dynamic routing protocol OSPF can not be used in a site if any of the PE interfaces linked to the site use IP unnumbered. The Routing Protocol on the Site dialog, **Connectivity** property page must be set to **None** or **EBGP**. Static routing is permissible.

You can indirectly associate a dynamic routing protocol (EBGP, RIP, OSPF, and EIGRP for Cisco) with a site containing an IP unnumbered interface.

To configure indirect association of a dynamic routing protocol with a site containing IP unnumbered interfaces:

1. Link the loopback interface that the IP unnumbered interface references to another site that has the desired routing protocol configured.

   The dynamic routing protocol applied to the loopback in the other site then applies to the IP unnumbered interface.

You can indirectly associate a dynamic routing protocol (EBGP, RIP, OSPF, and EIGRP for Cisco).

To indirectly associate a dynamic routing protocol with a site containing an IP unnumbered interface:

1. Link a loopback interface to a second site that has the desired routing protocol configured on it.
2. Refer to that loopback from the IP unnumbered interface in the first site.

Error Messages and Warnings

An attempt to configure an interface's Private PE IP to IP unnumbered when the site has a PE-CE routing protocol or routing protocol other than EBGP configured will trigger the following error:

```
<object_id>, IP Unnumbered cannot be set if the site uses a Routing Protocol other
than EBGP.
```

Configuring IP unnumbered on an unsupported interface type triggers the following error:

```
<object_id>, IP Unnumbered is not allowed for this type of Interface.
```

Few interface types support only IP unnumbered on their sub-interfaces (Frame Relay and ATM). An attempt to configure IP unnumbered on main (point-to-multipoint) interfaces will trigger the following error:

```
<object_id>, IP Unnumbered is not allowed for main interfaces of this type.
```

If the loopback used for the IP unnumbered address is removed from a device, the following fault is raised in the fault pane:

```
Site private PE ip unnumbered reference is invalid.
```

Supported Interface Types for IP Unnumbered

IP unnumbered can be configured on the following serial point-to-point interface (as reported during discovery):

- ds1 (18)
- e1 (19)
- propPointToPointSerial(22)
- ppp (23)
- ds3 (30)
- frameRelay (32)
- atm (37)
- sonet (39)
- frameRelayService (44)
- v35 (45)
- aa15 (49)
- async (84)
- pppMultilinkBundle (108)
- hdlc (118)
- tunnel (131)
- atmSubInterface (134)

- rfc1483 (159)
- aal2 (187)

Attempting to configure IP unnumbered on an unsupported interface type will trigger an error as described in "Error Messages and Warnings".

Restriction, Hints, and Tips

Before a loopback interface can be assigned to an IP unnumbered interface configuration:

- It must be created.
- An IP address assigned to it.
- It must be discovered.

The loopback can also be created in the same transaction in which you are using it.

> **Note:** Switching an interface from an explicit private PE IP address and mask to IP unnumbered and back does not affect its connectivity into the VPN - the interface continues to belong to the VRF.

You must have bridging configured for ATM devices to use IP unnumbered. The specific bridging protocols are device specific. Refer to the vendor documentation for your devices for details.

Sample Configuration

```
interface ATM0/0/0.4 point-to-point
ip unnumbered Loopback1
no ip directed-broadcast
no ip route-cache
atm route-bridged ip
pvc 4/100
encapsulation aal5snap
```

Setting Advanced VRF Table Options

Advanced options give you finer control of the VRF table and route handling within the VPN.

The following options are available:

- Specify whether the VRF table name and RD number are unique to the site or inherited from the VPN in which the site participates.
- For information on using site-specific or VPN-wide VRF details, see "Using VPN-wide or Site-Specific VRF Details".
- If using site-specific VRF and RD settings, specify whether to use the IP Service Activator default or a user-defined VRF table name.

Note: By specifying a user or system-defined RD number or VRF table name, you can control how IP Service Activator handles manually preconfigured VRF tables. For more information, see "Options for Handling VRF Tables".

For information on how user-defined VRF table names affect IP Service Activator's VRF reduction process, see "VRF Re-use and Reduction".

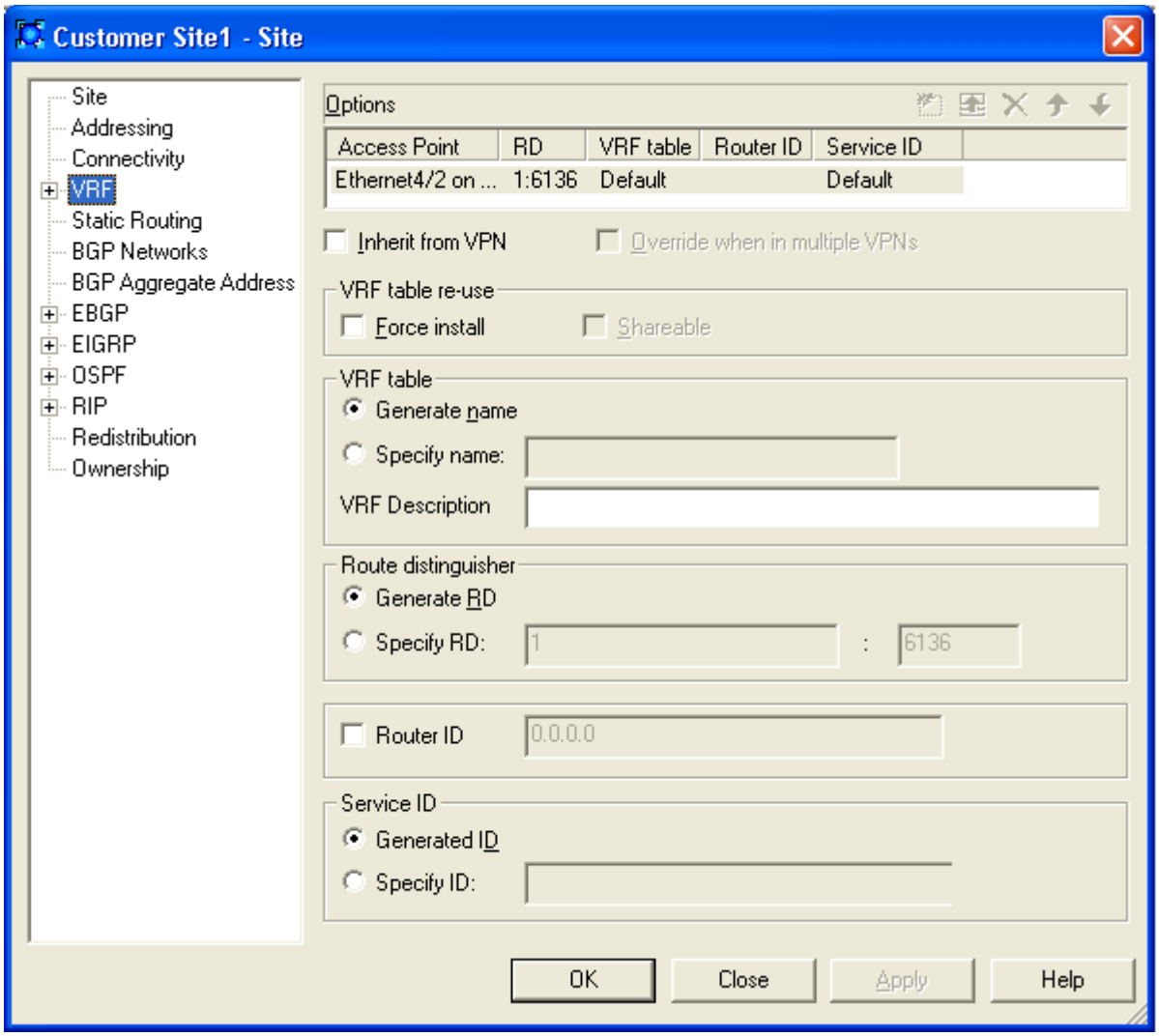
- Control over the VRF table. You can specify whether every interface associated with a site has its own VRF table, or can be merged with the VRF table for another interface where routes in the table are identical.
- Specify a manually preconfigured route map that filters the routes exported from one site to PE peers within the VPN.
- Specify the maximum number of routes from a CE router that can be added to the VRF table. The maximum may be set for the site or inherited from the default defined for the domain. A warning message may be logged when the number of routes stored reaches a user-defined percentage of the maximum.

For more information about advanced VRF options, see IP Service Activator online Help.

To set advanced VRF table options:

1. Display the Site dialog box and select the **VRF** property page, as shown in Figure 1–6.

Figure 1–6 The VRF Property Page

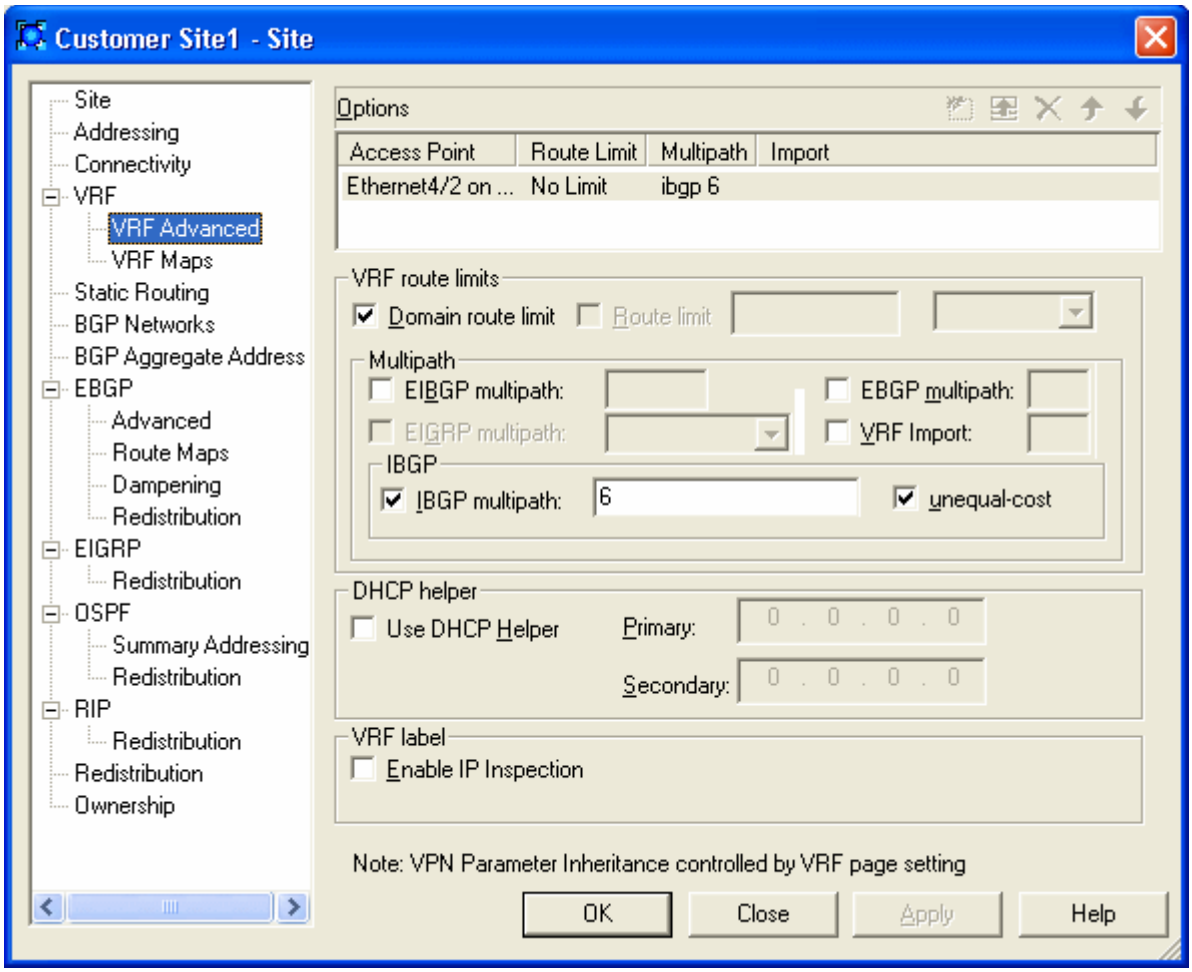


Any PE interfaces or sub-interfaces that you have linked to the site are listed. If no PE interfaces or sub-interfaces have been linked to the site, no addresses appear.

2. Specify values for each listed PE interface or sub-interface including I**nherit from VPN**, **Override when in multiple VPNs**, **Force install**, **Shareable**, **Generate name** or **Specify name**, **Generate RD** or **Specify RD**, **Router ID**, **Generated ID** or **Specify ID**, and **VRF Description**.

3. Under VRF, select the **VRF Advanced** property page, as shown in Figure 1–7.

Figure 1–7 The VRF Advanced Property Page



4. Specify values for each listed interface including **Domain route limit**, **Route limit**, **EIBGP multipath**, **EIGRP multipath**, **EBGP multipath**, **VRF Import**, **IBGP multipath**, **Use DHCP Helper**, and **Enable IP inspection**.

   Note: **Use DHCP Helper** is not supported on Juniper ERX.

5. Select the unequal-cost check box to allow unequal cost load balancing by selecting iBGP paths that do not have an equal cost.

To specify VRF import and export maps:

1. Display the Site dialog box, and under VRF, select the **VRF Maps** property page.

   Any PE interfaces that you have linked to the site are listed. If no PE interfaces have been linked to the site, no addresses appear.

2. For each listed PE interface, specify values including **Export map name** and **Import map name**:

   - Selecting **Export map name** allows the specification of an export map name for the VRF selected in the Export map list.
   - Selecting **Import map name** allows the specification of an import map name for the interface selected in the VRF Map list.

VRF Route maps can also be configured through the use of the **vrfRoutePolicy** configuration policy and referenced in the same way you would reference a manually configured route map.

Applying the **vrfRoutePolicy** configuration policy (at the Site level, for example) creates the route map but does not apply it to the site. Once the configuration policy is applied, you must still refer to it in the inbound/outbound fields of the Site dialog box for it to have any effect.

The **vrfRoutePolicy** configuration policy can refer to prefix lists, which can in turn be configured using the prefixListEntries configuration policy.

Refer to *IP Service Activator QoS User's Guide* for details on installing and applying configuration policies.

For details about the configuration policies, see the IP Service Activator online Help. The Configuration Policy - vrfRoutePolicy topic contains details on the fields available in this configuration policy.

Note: VRF Import is not supported on Juniper ERX devices.

Setting Network and Aggregate Statements

In the Site properties dialog box, you can access the **BGP Networks** and **BGP Aggregate Address** property pages to set up network and aggregate statements.

Note: BGP Networks and BGP Aggregate Address are supported on Cisco but not on Juniper ERX.

Network statements are used to advertise networks to other routers. For the information to be advertised by BGP, a route to the specified network must be present in the routing table. This routing information can come from connected routers and dynamic routing or static routing sources.

Aggregate statements summarize routes into a single advertisement that is sent to BGP peers.

For more detailed, conceptual information on network and aggregate statements, see *IP Service Activator Cisco IOS Device Support Guide*.

Specifying Metrics for Route Redistribution

You can specify the metric to apply to routes distributed from the selected PE-CE routing protocol into other Internal Gateway Protocols (IGPs) and BGP, and vice versa.

To avoid introducing routing loops and convergence problems, you can filter and refine the redistribution of routes by associating a preconfigured route map through preconfigured configuration policies, or policy statement, with redistributed routes.

Directly-connected networks can also be redistributed into routing protocols. IP Service Activator supports direct redistribution of connected routes.

The default route may also be distributed through iBGP to peers within the VPN.

To specify metrics for route redistribution:

1. In the Site properties dialog box, select the **Redistribution** property page.
2. Deselect the **Use default redistribution** check box.

The **Metric** and **Policy** fields that are enabled on the **<Destination-protocol> Redistribution** property pages depend on the protocol selected for PE-CE connectivity.

Note: If the **Use default redistribution** check box is selected, the IP Service Activator default metrics will be used. Otherwise, the metric, and policy attributes for redistribution of connected routes can be specified in the redistribution matrix.

---

3. Select one of the following <Destination-protocol> Redistribution pages:
   - EBGP
   - EIGRP
   - OSPF
   - RIP
4. If you wish to specify a metric or route map for connected routes, select the **Enable Connected** check box.
5. Provide values for the fields in each column for each connectivity type as required.

   For example, on the **EBGP Redistribution** property page:
   - **Metric**: The metric to apply to routes learned from the PE-CE protocol as they are redistributed into BGP.
   - **Policy**: The name of a manually preconfigured route map or, for Juniper M-series devices, policy statement to apply to routes distributed into BGP.

   On the other <Destination-protocol> Redistribution property pages:
   - <*Protocol*> **Metric**: The protocol-specific metric to apply to routes distributed from another protocol into the protocol used for PE-CE connectivity.
   - <*Protocol*> **Policy**: The name of a manually preconfigured route map or, for Juniper M-series devices, policy statement to apply to routes distributed from another protocol into the protocol used for PE-CE connectivity.
6. If you wish to distribute the default route through iBGP to peers, select the Enable Default Route check box.
7. Click the **Set** button (shown in Figure 1–8) to confirm your changes.

Figure 1–8 The Set Button

8. Click **OK** to commit the changes and close the dialog box.

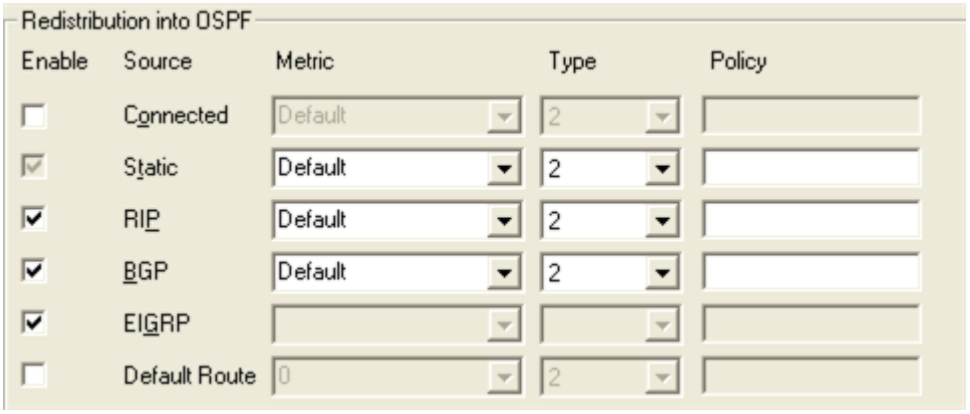
Note the following hints and tips:

- On the **OSPF Redistribution**, **RIP Redistribution**, and **EIGRP Redistribution** property pages, only the value entered for BGP affects device configuration. A value specified for redistribution from any other protocol affects configuration only where two or more interfaces on the PE device participate in the same VPN, use different protocols for PE-CE connectivity and share the same VRF table.
- The RIP metric is based on hop count. The maximum valid discrete metric is **15**. A value of **16** is considered infinite.

- If no values are specified on a **<Destination-protocol> Redistribution** property page, the device vendor default metrics are used.

As an example, with OSPF selected as the connectivity type, the column headings going across the redistribution matrix are interpreted as shown in Figure 1–9.

Figure 1–9 OSPF Redistribution Matrix Columns



Setting Up OSPF Properties for a Site

To set up OSPF properties for a site:

1. Display the Site dialog box and select the **OSPF** property page.
2. Any PE interfaces or sub-interfaces that you have linked to the site are listed. If no PE interfaces or sub-interfaces have been linked to the site, no addresses appear.
3. Specify OSPF settings for each listed PE interface or sub-interface including **Area**, **Distribute in filter**, and **Distribute out filter**.
4. From the Area Type list, select the **OSPF** Area Type on Cisco/Brocade equipment. Area Type selections other than **Normal** are applicable only to OSPF instances configured within the context of a VRF.
   - If **Normal** is selected, the site connects to normal OSPF Area functionality.
   - If **Stub** is selected, the site connects to a Stub Area. Stub Areas do not accept external summary routes, or LSA type 4 or 5 packets.
   - If **Totally Stub** is selected, the site connects to a Totally Stubby Area. A Totally Stubby Area does not accept any external summary LSAs, or LSA type 3, 4 or 5 packets.
   - If **NSSA** is selected, the site connects to a Not So Stubby Area (NSSA) with a default route advertised into the site. With this selection, the Default Route into the site must be explicitly configured on the **Redistribution into OSPF** property page.
   - If **NSSA (Totally Stub)** is selected, the site connects into a Not So Stubby Area (NSSA) Totally Stub area with a default route advertised into the site and metric set. With this selection, the Default Route into the site is automatically generated as a Type 3 LSA. This Area Type is not supported on Brocade.
5. Select **No NSSA Type 7 Redistribution** to suppress NSSA behavior in which Type 7 LSAs are translated to Type 5 LSAs. With this selected, no translation will occur.

6. Under Spf Throttling, enable control of timing and execution of SPF recalculations by selecting **Enable**. If **Enable** is selected, you can specify the values in **Min delay**, **Holdtime**, and **Max delay** fields.
7. Specify the maximum redundant routes OSPF can use by selecting Maximum paths. The range of values is from 1 through 6.
8. Specify the cost of sending a packet on the selected interface by selecting **Cost**. Enter a value in the range from 1 to 65,535.
9. Enable the use of the tag value to identify routes redistributed into OSPF from BGP by selecting **BGP redist tag**. The value used is specified in the accompanying field.
10. Under MD5 Authentication, do one of the following:
    - Select **Inherit from VPN**. This inherits the interface's OSPF authentication settings from the parent VPN. Deselecting it allows for no authentication and allows selection of the **Enable** check box for MD5 Authentication.
    - Select **Enable**. This enables MD5 key authentication for OSPF for the selected interface. Entering the MD5 key in the Key field lets you use and re-enter it in the Confirm Key field.
11. Under Process ID, specify the ID of an OSPF process for the selected interface by selecting **Generated ID** or **Specify ID**. Selecting **Specify ID** lets you enter a value in the range from 1 to 65535.

There are additional details available on OSPF Area Types and MD5 Authentication in the IP Service Activator online Help.

Setting Up OSPF Summary Addressing

To set up OSPF Summary Addressing for a site:

1. Display the Site dialog box and under OSPF, select the **Summary Addressing** property page.

   Any PE interfaces or sub-interfaces that you have linked to the site are listed. If no PE interfaces or sub-interfaces have been linked to the site, no addresses appear.
2. Specify values for each listed PE interface or sub-interface including **IP Address**, **Mask**, **Suppress Advertise**, and **Use this tag**.

Setting Up RIP Properties for a Site

To set up a site's RIP properties:

1. Display the Site dialog box and select the **RIP** property page.

   Any PE interfaces or sub-interfaces that you have linked to the site are listed. If no PE interfaces or sub-interfaces have been linked to the site, no addresses appear.
2. Configure the following for each listed PE interface or sub-interface:
   - **Ignore Routes From**
   - **Passive Interface**

There is detailed information available on these two panels in the IP Service Activator online Help.

Note: On Cisco and Brocade devices, the RIP version is always configured as version 2.

Setting Up EIGRP Properties for a Site

To set up a site's EIGRP properties:

1. Display the Site dialog box and select the **EIGRP** property page.

   Any PE interfaces or sub-interfaces that you have linked to the site are listed. If no PE interfaces or sub-interfaces have been linked to the site, no addresses appear.

2. Configure the MD5 Authentication for each listed PE interface or sub-interface.

The EIGRP ASN settings are configured on the **Site properties - Connectivity** property page.

MD5 Authentication

Use this panel to enable MD5 Authentication.

To inherit the interface's EIGRP authentication settings from the parent VPN:

1. Select the **Inherit from VPN** check box

   The default settings for the VPN can be set on the **VPN properties - Connectivity** property page.

To allow selection of the **Enable check box for MD5 Authentication**, or for no authentication:

1. Deselect the **Inherit from VPN** check box.

EIGRP MD5 Authentication uses Key Chains which must be present on the device either through previous manual configuration, or through the keychains configuration policy.

Setting Up the VPN

In order to set up a VPN, you need to create a VPN object and link the appropriate sites to it.

Applying QoS to CE Devices or SAA/Configured Services to a VPN

If you need to apply QoS to CE devices, or SAA or other IP Service Activator-configured services to a VPN, the order of setup tasks is significant and must be as follows:

- Create a management VPN and propagate it to the network.

  The management VPN type provides control of the CE devices.

- Create the fully-meshed or hub and spoke customer VPN and propagate it to the network.

- Apply QoS, SAA, or other IP Service Activator-configured services to the fully-meshed or hub and spoke customer VPN.

For an outline of the steps required to set up a management VPN, see Appendix A.

Note: The best practice to use when removing a VPN to which QoS, SAA, or other IP Service Activator-configured service has been applied, is to remove the policy, measurement, or other IP Service Activator-configured services before deleting the VPN.

Creating an MPLS VPN

VPNs are created for IP Service Activator customers – you cannot create an MPLS VPN that is customer-independent. For information on creating customers, see "Setting Up Customers".

For more information about creating an MPLS VPN, see the IP Service Activator online Help.

To create a VPN:

1. On the **Service** tab, open the relevant customer folder and select the **VPNs** folder.
2. Right-click and select **Add VPN** from the context menu.

   The VPN dialog box opens.
3. Specify values including **Name**, **Remarks**, **Level**, and **VPN Protocols**.
4. Select the Address Family from the drop-down list. You can select **IPv4** or **IPv6**.
5. Select the **Connectivity** property page and specify the **Connectivity Type**:
   - **Mesh**: Each site can communicate with all other sites.
   - **Hub and Spoke**: One or more sites act as a controlling interface.
   - **Management**: Hub and spoke topology that provides connectivity to the CE device where QoS or SAA will be implemented on the VPN.

   If you are setting up a hub and spoke or a management VPN you can specify that at least one of the sites is defined as a hub. For more information, see "Specifying a Hub Site".

Setting Route Target Numbers

The import and export policies of a VRF table are defined by route target (RT) numbers. An import policy only allows iBGP routes whose RTs match the RTs of the import policy to be imported into the VRF table. An export policy specifies which RTs are attached to iBGP routes exported from the VRF.

By default, IP Service Activator automatically creates two RT numbers per VPN called **Default** and **Default+1**.

The Default value is based on the domain's Autonomous System Number (ASN) and the unique object ID assigned to the VPN by IP Service Activator. By default, this value defines the import and export policies of all sites if the VPN is fully-meshed (**Mesh**), or the import and export policies of the hub site if the VPN is a hub and spoke or management VPN.

The **Default+1** value is the Default value incremented by 1. By default, this value defines the import policy of all hub sites and the export policy of all spoke sites if the VPN is a hub and spoke or management VPN. This value is not used if the specified VPN connectivity is **Mesh**.

You can define additional RT numbers, and assign to each RT number any combination of import/export policy and site behavior.

IP Service Activator supports **Custom** or user-defined RT numbers in the following formats:

- *ASN*:*Number* where *ASN* is an integer from 1 to 65,535 and *Number* is an integer from 1 to 4,294,967,295.
- *IP_Address*:*Number* where *IP_Address* is an IP address and *Number* is an integer from 1 to 65,535.

> **Note:** IP Service Activator checks that system-generated RT numbers are unique. However, no such check is made on user-defined RT numbers and non-unique numbers are permitted.

To define and allocate an RT number:

1. Display the VPN dialog box and select the MPLS property page.
2. Specify the Route Target. Select from **Default**, **Default+1** or **Custom**.

   For information about Route Target values, see "Setting Route Target Numbers".
3. Specify values including **Hub**, **Spoke** and **Mesh**. Select from **None**, **Import**, **Export** or **Both**.
   - If **None** is selected, the RT value is not used.
   - If **Import** is selected, the site will import iBGP routes tagged with the specified RT value. This is the default for spoke sites in a fully-meshed VPN and for hub sites in a hub and spoke or management VPN.
   - If **Export** is selected, the site will attach the specified RT value to export iBGP routes. This is the default for spoke sites in a hub and spoke or management VPN.
   - If **Both** is selected, the site will import iBGP routes tagged with the specified RT number and attach the RT value to exported iBGP routes. This is the default for hub sites in a hub and spoke or management VPN and all sites in a fully-meshed VPN.
4. Select the **Vrf-Target (JUNOS only)** check box if appropriate. When selected, the Juniper JUNOS cartridge will generate VPN configuration using the VRF-Target format. This selection applies to the selected Route Target in the above list. See the Online Help for more details.
5. Click **Apply**.

Linking Sites to the VPN

Create the VPN by linking the appropriate customer sites to the VPN object. A site can be in more than one VPN and can be a hub in one VPN and a spoke in another. A site can be a spoke in more than one VPN.

To link a site to a VPN:

1. Drag and drop the site object onto the VPN to create a link.

   If the VPN is a hub and spoke or management VPN, added sites are spokes by default.

Note: On device driver technology, problems occur if spoke sites with separate VRF tables on a single PE device are added to a fully-meshed VPN while the device driver is down. The next time a transaction is committed after the driver has re-started the PE device is put into the 'Intervention Required' state and an error is raised. The problem does not occur if the VPN topology change is made after the device driver has re-started, however.

Using an RD Number per VPN or per Site

By default, IP Service Activator automatically generates a site-specific VRF table name and RD number for each site that participates in a VPN.

At the VPN level, you can override the IP Service Activator default by specifying that the same VRF table name and RD number is applied to all sites that participate in the VPN. You can choose whether to use IP Service Activator-generated values or specify your own VRF table name and/or RD number.

Note: If you wish to use this feature, in addition to setting a VPN-level option you must also select the **Inherit from VPN** option in each relevant site's property pages. For more information, see "Setting Advanced VRF Table Options".

Using a single RD number for all sites in a VPN is suitable only where a site belongs to one intranet VPN. If the site may become a member of an extranet VPN in the future, this method is not recommended.

Use the **Override when in multiple VPNs** option for more control over how RD numbers are assigned. If both **Inherit from VPN** and **Override when in multiple VPNs** are selected:

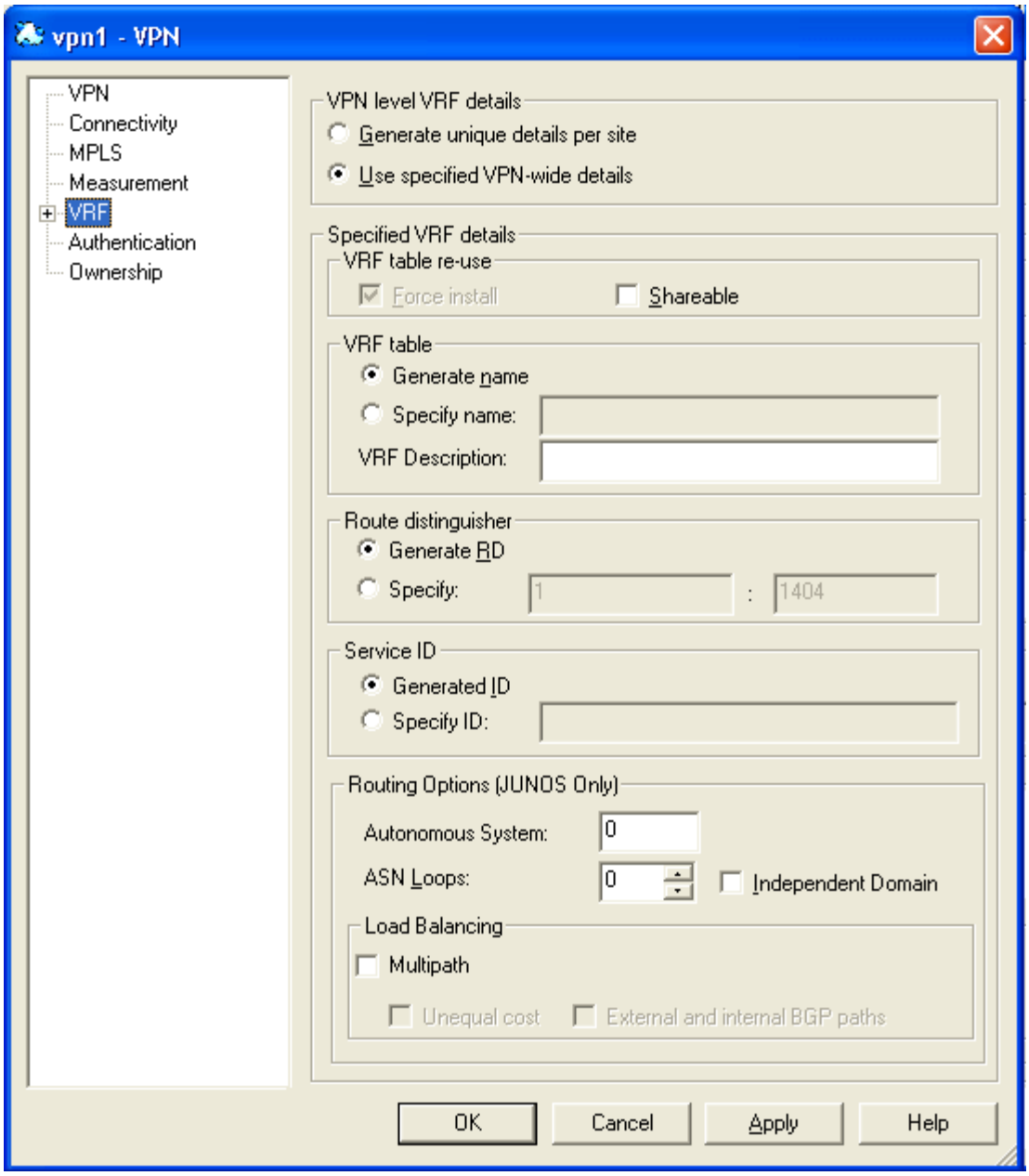
if the site is a member of only one VPN, the VRF table name and RD are derived from the parent VPN

if the site is a member of multiple VPNs, the VRF table name and RD are derived using the site specific options

To use the same RD number for all sites in a VPN:

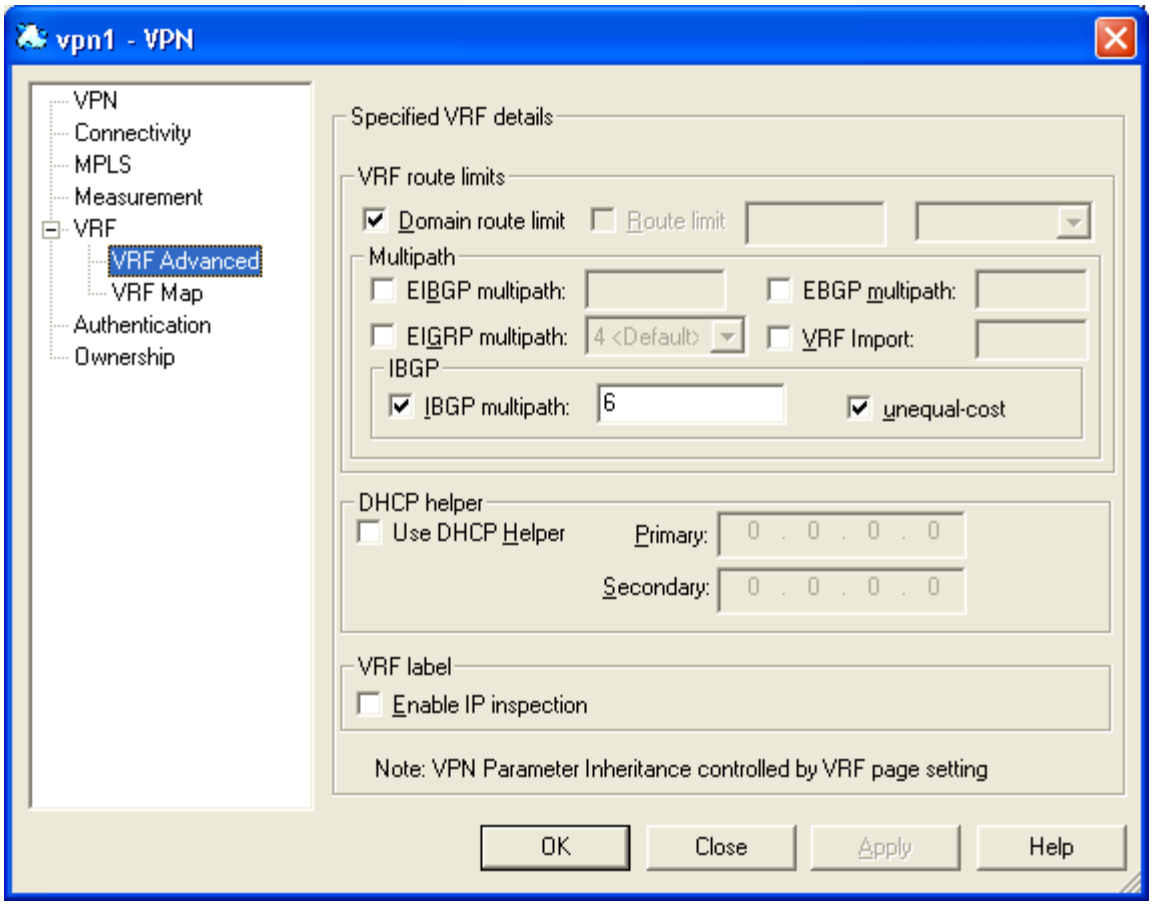
1. Display the VPN dialog box and select the **VRF** property page, as shown in Figure 1–10.

Figure 1–10 The VRF Property Page



2. Select **Use specified VPN-wide details**.
3. Select values including **Force install**, **Shareable**, **Generate name**, **Generate RD**, and **VRF Description**.
4. Under VRF, select **VRF Advanced** property page, as shown in Figure 1–11.

Figure 1–11 VRF Advanced Property Page



5. Select **Domain route limit**, **Route limit**, **EIBGP multipath**, **EBGP multipath**, **EIGRP multipath**, **VRF Import**, **IBGP multipath**, **Use DHCP helper**, and **Enable IP inspection**.

> **Note:** **Use DHCP Helper** is not supported on Juniper ERX.

6. Select the **unequal-cost** check box to allow unequal cost load balancing by selecting iBGP paths that do not have an equal cost.
7. The VRF description can also be set at the Site level. See "Setting Advanced VRF Table Options".

Specifying a Hub Site

If you are setting up a hub and spoke or management VPN, you can specify one or more sites as the hub site.

To specify that a site is a hub:

1. From the VPN context menu, select **Properties** and select the **Connectivity** property page.

   Sites that have been added to the VPN are listed on the page.
2. In the Connectivity field, select **Hub and Spoke** or **Management** from the drop-down menu.

3. To specify that a site is a hub, select the check box next to the relevant site's name in the Hub Sites in VPN panel.

Creating a VPN Map

Each VPN can be shown as a map view, which shows the sites within the VPN. You can choose whether the sites are laid out automatically or arrange them manually. In the manual layout option, you can specify whether objects snap to a grid layout and the granularity of the grid. The default is manual layout.

To display the VPN map:

1. Double-click on the relevant VPN in the Hierarchy pane.

   A representation of the VPN is shown in the Details pane. Initially it consists of the VPN object only. Sites linked to the VPN are listed in the palette.

To specify layout options for a VPN map:

1. If no map exists for this VPN, then from the VPN icon's pop-up menu, select **Add Map View**.
2. Add the map name. Optionally, you can also add a description, change the zoom level, and deselect **Default Palette Visible**.
3. If a map exists for this VPN, in the Details pane in Map View, right-click the background and select **Properties**.

   The Map View dialog box opens.

   Note: If a map has a background image, you may need to click on the map's tab at the bottom of the Details pane to display its context menu.

4. Select the **Layout** property page.
   - If you want to lay out sites manually, select **Manually lay out items on map**.
   - To specify that sites snap to a grid, select the **Snap to grid** option and specify the granularity of the Grid in millimeters.
   - If you want to lay out sites automatically, select **Automatically lay out items on map** and select items to be shown including **Networks**, **Sites**, **Devices**, **Interfaces**, **VCs**, **VC End Points**, and **Segments**.
   - You can specify **Max nodes**, **Max fan** and **Max Devices** values to control the automatic layout. For information about these settings, see *IP Service Activator User's Guide* and IP Service Activator online Help.
5. Click **OK**.

   If you specified automatic layout, all previously unmapped sites are added to the VPN map.

Listing the Sites in a VPN

You can list the sites that are associated with a VPN and display summary information for each site.

To list the sites in a VPN:

1. Select the relevant VPN from the hierarchy tree or the topology map.

2. On the toolbar, click the **Report View** button.

   IP Service Activator lists the sites that are associated with the VPN and displays the properties for each site.

Implementing the VPN

After the site and VPN details are set up and the relevant devices are managed, the entire configuration can be applied by committing the transaction.

When you commit the transaction, any concrete VPNs that will be created are listed in the Concretes property page of the Transaction dialog box.

Any validation errors are reported in the Fault property page of the Transaction dialog box and the Current Faults pane.

To cancel the transaction after reviewing the concrete VPNs that will be created and the faults generated by the transaction, click **Cancel**.

To proceed with the transaction, click **OK**. Configuration details are sent to the proxy agent/Network Processor and on to the appropriate device driver/cartridge. For information about committing a transaction, see *IP Service Activator User's Guide*.

Use the built-in transaction status monitoring feature to track the provisioning status of the transaction. Optionally, once the transaction is provisioned successfully, if the device is managed by the Network Processor, you can perform a device audit.

For details on transaction monitoring, and performing audits, see *IP Service Activator Administrator's Guide*.

Viewing Implemented VPNs

You can view a list of the VPNs that have been propagated to the network and installed on an interface or subinterface.

To view implemented VPN details in the IP Service Activator client:

1. In the Hierarchy pane, select the **Service** tab.
2. Expand the Customer folder and select the required customer from the displayed customer list. The list of related sites and VPNs is displayed.
3. Expand the VPNs folder. The list of implemented VPNs is displayed.
4. Double-click the required VPN. The Details pane for that VPN is displayed on the right.
5. In the Details pane, click the **VPNs** tab to view VPNs implemented on the selected object. All concrete VPNs appear on a yellow background.

   VPN details are listed under the following headings:

   - **VPN**: name of the VPN
   - **Site**: the site associated with the VPN
   - **Access Point**: the interface or sub-interface associated with the site
   - **Device**: this column remains blank for MPLS VPNs
   - **State**: current state of the VPN:
     * **Inactive**: the VPN has been created but has not been propagated to the proxy agents

    - **Active**: the VPN has been propagated to the proxy agents
    - **Rejected**: the VPN configuration was rejected
    - **Installed**: VPN configuration has been installed on the designated device
- **Conflict**: there is a configuration error in the VPN
- **ID**: internal ID number by which the VPN is identified.

Viewing the Statistics Summary

You can see the inactive, active, installed, and failed states by viewing the Statistics Summary.

To view the Statistics Summary:

1. When the Details pane for an implemented VPN is open, click **View** in the menu bar.
2. Select **Statistics Summary**. The Statistics Summary for that VPN is displayed at the bottom of the Details pane.

2

Setting Up Layer 3 Multicast Services

This chapter describes Oracle Communications IP Service Activator's implementation of multicast services. The chapter includes information about Multicast, IP Multicast Services, and VPN Multicast Services.

About Multicast

Multicast provides an efficient means of transmitting the same data to multiple receivers in a multicast group. A multicast group is an arbitrary number of receivers that join a group in order to receive a particular traffic. This multicast group has no physical or geographical boundaries; the hosts (sources or receivers) can be located anywhere on the Internet or on any private internetwork. A group of receivers can listen to a single address, or a group of addresses.

Multicast uses the class D address range running from 224.0.0.0 through 239.255.255.255. The addresses do not have a subnet mask length associated with them for forwarding purposes. Each address is treated independently so the subnet mask used for forwarding is always assumed to be /32.

Applications that take advantage of multicast include video conferencing, corporate communications, distance learning, and software distribution.

IP Service Activator supports two Layer 3 multicast services:

- IP multicast
- VPN multicast

IP Service Activator configures multicast using configuration policies.

About IP Multicast Services

IP multicast refers to the implementation of multicast communication on the Internet.

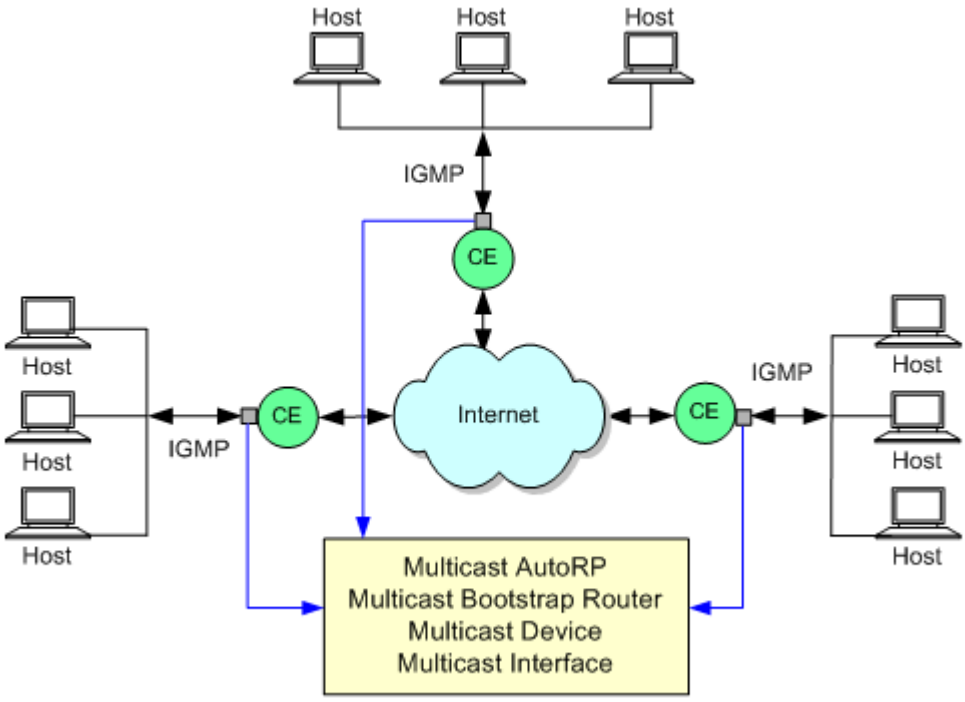
Hosts in a multicast group that are interested in receiving data from a source to a particular group join that group using Internet Group Management Protocol (IGMP).

IP Service Activator supports configuration policy-based activation of IP multicast on Customer Edge (CE) routers. This includes the configuration of multicast RPs using static configuration, Auto-RP, or Bootstrap Router (BSR). Configuration of both Protocol Independent Multicast Sparse Mode (PIM-SM) and Protocol Independent Multicast Source Specific Multicast (PIM-SSM) are supported as well as activation of IGMP, Cisco Group Management Protocol (CGMP), and Router-Port Group Management Protocol (RGMP) on LAN interfaces.

IP multicast is configured on CE interfaces and is supported on specific Cisco IOS devices. Support can be extended to other devices using IP Service Activator Software Development Kit (SDK).

Figure 2–1 illustrates the configuration of IP multicast services on CE interfaces.

Figure 2–1 IP Multicast Services on CE Interfaces



Prerequisites for Configuring IP Multicast

In the IP Service Activator client, load the **IPMulticastPolicyTypes.policy** and **MulticastInterfacePolicyTypes.policy** policy files in order to configure IP multicast. For information on loading configuration policies, see *IP Service Activator QoS User's Guide*.

Once the .policy files are loaded, the following configuration policies will be available for configuration on the CE interface:

- **Multicast AutoRP**: configures multicast RPs using the Auto-RP mechanism
- **Multicast Bootstrap Router**: configures multicast RPs using the BSR mechanism
- **Multicast Device**: enables and configures IP multicast on a device
- **Multicast Interface**: enables and configures IP multicast on a CE interface

Multicast Routing Protocols

Multicast routing protocols distribute data to multiple recipients. Using IP multicast, a source can send a single copy of data to a single multicast address, which is then distributed to an entire group of recipients.

IP Service Activator supports the following routing protocols that implement IP multicast routing:

- IGMP
- Protocol Independent Multicast (PIM): There are three PIM modes:
  - Dense mode (DM): Delivers data to the receivers without the receivers' request.
  - Sparse mode (SM): Only network segments with active receivers that have explicitly requested the data will receive the traffic.
  - Sparse-Dense mode (SDM): Allows individual groups to be run in either sparse or dense mode, depending on whether RP information is available for that group. If the router learns RP information for a particular group, it will be treated as sparse mode; otherwise, that group will be treated as dense mode.
- CGMP
- RGMP

About Rendezvous Points

A rendezvous point (RP) acts as a meeting place for sources and receivers of multicast data. A router performs this role when operating in PIM-SM.

In a PIM-SM network, sources must send their traffic to the RP. This traffic is then forwarded to the receivers down a shared distribution tree. By default, when the first hop router of the receiver learns about the source, it will send a Join message directly to the source, creating a source-based distribution tree from the source to the receiver. This source tree does not include the RP unless the RP is located within the shortest path between the source and receiver.

By default, the RP is needed only to start sessions with sources and receivers. Consequently, the RP experiences little overhead from traffic flow or processing.

IP Service Activator supports the following RP mechanisms:

- Static RP
- Auto-RP
- Bootstrap Router (BSR)
- Protocol Independent Multicast Source Specific Multicast

Static RP

Static RP: a mechanism to configure the address of the RP on every router in the domain. In PIM-SM version 1, all routers directly connected to sources and receivers were required to manually configure with the IP address of the RP. It is simple to configure Static RPs in a small network, but can be laborious in a large and complex network.

For information on configuring a multicast CE with PIM-SM, refer to the topics "Activating Multicast CE with PIM Sparse Mode and a default Static RP" and "Activating Multicast CE with PIM Sparse Mode and a set of Mapped Static RPs" in the IP Service Activator Online Help.

Auto-RP

Auto-RP is a mechanism to automate distribution of RP in a multicast network. For Auto-RP to work, a router must be designated as an RP-mapping agent, which receives the RP-announcement messages from the RPs and arbitrates the conflicts. The RP-mapping agent then sends the consistent group-to-RP mappings to all other

routers. All routers automatically discover which RP to use for the groups they support.

The benefits of Auto-RP are as follows:

- Easy to serve different groups with the use of multiple RPs within a network.
- Allows load-splitting among different RPs and arrangement of RPs according to the location of group participants.
- Avoids inconsistent, manual RP configurations that can cause connectivity problems.

> **Note:** If you configure PIM in sparse mode or sparse-dense mode and do not configure Auto-RP, you must statically configure an RP.
>
> If router interfaces are configured in sparse mode, Auto-RP can still be used if all routers are configured with a Static RP address for the Auto-RP groups.

Auto-RP can co-exist with Static RP. Auto-RP takes precedence over Static RP. If a router receives Auto-RP information for a multicast group that has Static RP configuration, the Auto-RP information will be used.

Auto-RP is not supported for IPv6 multicast.

For information on configuring a multicast CE with PIM Sparse or Sparse-Dense modes, refer to the IP Service Activator Online help.

Bootstrap Router

Bootstrap Router (BSR) is a mechanism for a router to learn RP information. The mechanism ensures that all routers in the PIM domain have the same RP cache as the BSR. It is possible to configure the BSR to help select an RP set from BSR candidate RPs. The function of the BSR is to broadcast the RP set to all routers in the domain. BSR is ideal for Sparse mode.

The BSR capability was added in PIM version 2. It automates and simplifies the Auto-RP process. By default, BSR is enabled in Cisco IOS releases supporting PIM version 2.

BSR and Auto-RP protocols must not be configured in the same network.

> **Note:** Auto-RP is a proprietary Cisco protocol. PIM version 2 with BSR is an IETF standards track protocol.

For information on configuring a multicast CE with a BSR mechanism, refer to the IP Service Activator Online help.

Static RP allows you to have only one RP per multicast group, whereas Auto-RP allows multiple RPs per multicast group. However, only one RP is used at a time. BSR's can be redundantly configured, although only one will be active at any time.

Protocol Independent Multicast Source Specific Multicast

Protocol Independent Multicast Source Specific Multicast (PIM-SSM) is an extension of the PIM protocol. Using this mechanism a client can receive multicast traffic directly from the source. PIM-SSM uses the PIM-SM functionality to create the shortest path tree (SPT) between the receiver and the source without the help of an RP.

For information about configuring a multicast CE with PIM-SSM, refer to the IP Service Activator online Help.

About VPN Multicast Services

VPN multicast provides the ability to support multicast over a Layer 3 Virtual Private Network (VPN). As Layer 3 VPNs support only unicast traffic connectivity, deploying this service in conjunction with a Layer 3 VPN allows service providers to offer both unicast and multicast connectivity to Layer 3 VPN customers.

VPN multicast allows an enterprise to transparently interconnect its private network across the network backbone of a service provider. The use of a VPN multicast to interconnect an enterprise network in this way does not change the way the enterprise network is administered, nor does it change general enterprise connectivity.

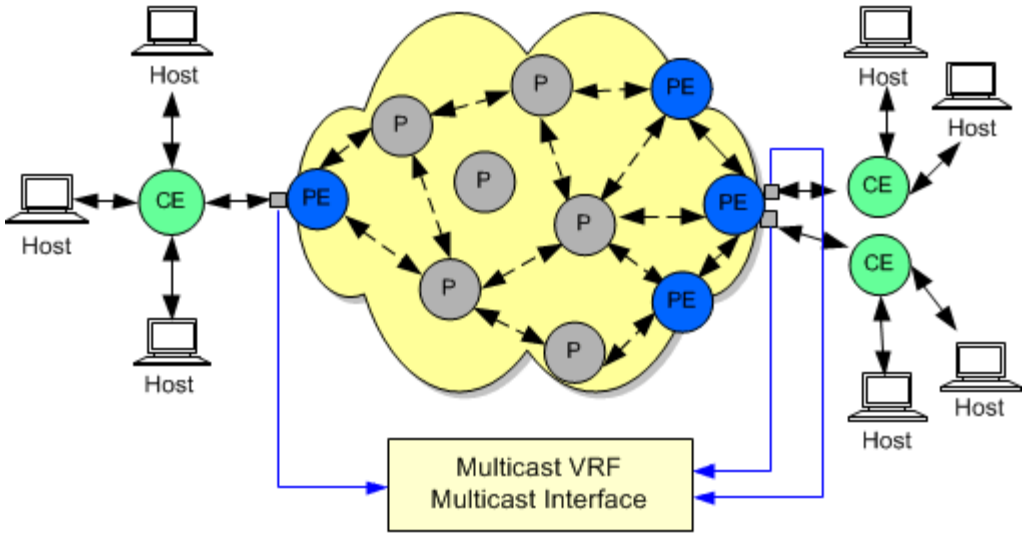
IP Service Activator supports:

- A set of policies that enable the creation of VPN multicast sites.
- Creating Access Lists when configuring VPN multicast. The access lists include:
  - PE-CE Access List and PIM
  - Mrinfo-filter
  - Static RP-to-Group mapping
  - PIM-SSM Range
  - SPT Threshold
- Enabling VPN multicast on a device
- Setting Rate-Limit on PIM-SM register messages
- Configuring the address of a PIM rendezvous point for a particular group
- Defining PIM-SSM range
- Specifying the threshold that must be reached before moving to the SPT

VPN multicast is configured on Provider Edge (PE) interfaces and is supported on Cisco IOS devices (specifically Cisco 7500 and 10,000 series). The support can be extended to other devices using IP Service Activator SDK.

Figure 2–2 illustrates the configuration of a VPN multicast service on PE interfaces.

Figure 2–2 VPN Multicast Services on PE Interfaces



Prerequisites for Configuring VPN Multicast

In the IP Service Activator client, load the **VPNMulticastPolicyTypes.policy** and **MulticastInterfacePolicyTypes.policy** files. For information on loading configuration policies, see *IP Service Activator QoS User's Guide*.

The following configuration policies will be available to you for configuration on the PE interface once the .policy files are loaded:

- Multicast VRF configures multicast on a VPN, VPN site or VPN interface
- Multicast Interface configures VPN multicast on a PE interface

About Multicast VRF

VPN multicast introduces multicast routing information to the VPN Routing and Forwarding table (MVRF). When a PE router receives multicast data or control packets from a CE router, forwarding is performed according to the information in the MVRF. VPN multicast does not use label-switching.

A set of MVRFs that can send multicast traffic to each other constitutes a multicast domain. For example, the multicast domain for a customer who wants to send certain types of multicast traffic to all global employees would consist of all CE routers associated with that enterprise.

About Multicast Distribution Tree

VPN multicast establishes a static default MDT for each multicast domain. The default MDT defines the path used by PE routers to send multicast data and control messages to every other PE router in the multicast domain. If Source Specific Multicast (SSM) is used as the core multicast protocol, the multicast IP addresses used for the default and data MDT must be configured within the SSM range on all PE and P routers.

VPN multicast also supports the dynamic creation of MDTs for high-bandwidth transmission. Data MDTs are unique to Cisco IOS software. Data MDTs are intended for high-bandwidth sources such as full-motion video inside the VPN to ensure

optimal traffic in the MPLS VPN core. The threshold at which the data MDT is created can be configured on a per-router or a per-VRF basis.

When the multicast transmission exceeds the defined threshold, the sending PE router creates the data MDT and sends a User Datagram Protocol (UDP) message, which contains information about the data MDT to all routers on the default MDT.

For information on activating VPN multicast on a VPN site and removing a site from the multicast domain, refer to the IP Service Activator Online help.

3

Setting Up Layer 2 Martini VPNs

This chapter describes how to set up Layer 2 Martini VPNs for Oracle Communications IP Service Activator.

About Layer 2 Martini VPNs

A Layer 2 Martini point-to-point connection is a Pseudo-Wire (PW) or tunnel configured between two endpoints across an IP network.

The connection uses MPLS labels to encapsulate and transport various Layer 2 data formats, including Ethernet (Port), Ethernet (VLAN), Frame Relay, ATM Cell, and ATM AAL5 across an IP network. The pseudo-wire provides a transparent connection, so users see no change in their Layer 2 data. (The pseudo-wire does not aim to meet QoS aspects of the connection, particularly in the ATM case.) The Layer 2 endpoints can be interfaces, sub-interfaces, or other endpoint identifiers (VCI/VPI on ATM, DLCI on Frame Relay, or VLAN ID on Ethernet).

A Layer 2 Martini VPN is an association of Layer 2 Martini point-to-point connections.

Benefits of Layer 2 Martini VPNs

Layer 2 Martini VPNs enable the encapsulation and transport of legacy data types over IP networks. As service providers upgrade their network core, connections between legacy networks can be maintained. Customers needing traditional connectivity over a third-party network can be served using the same IP core network, regardless of the packet types they need to transport. Additionally, the pseudo-wire saves the complexity of carrying the customers routes across the network.

Support of Ethernet technologies permits operators to use inexpensive Metro- Ethernet solutions in the local area network, reducing the rollout cost of new networks.

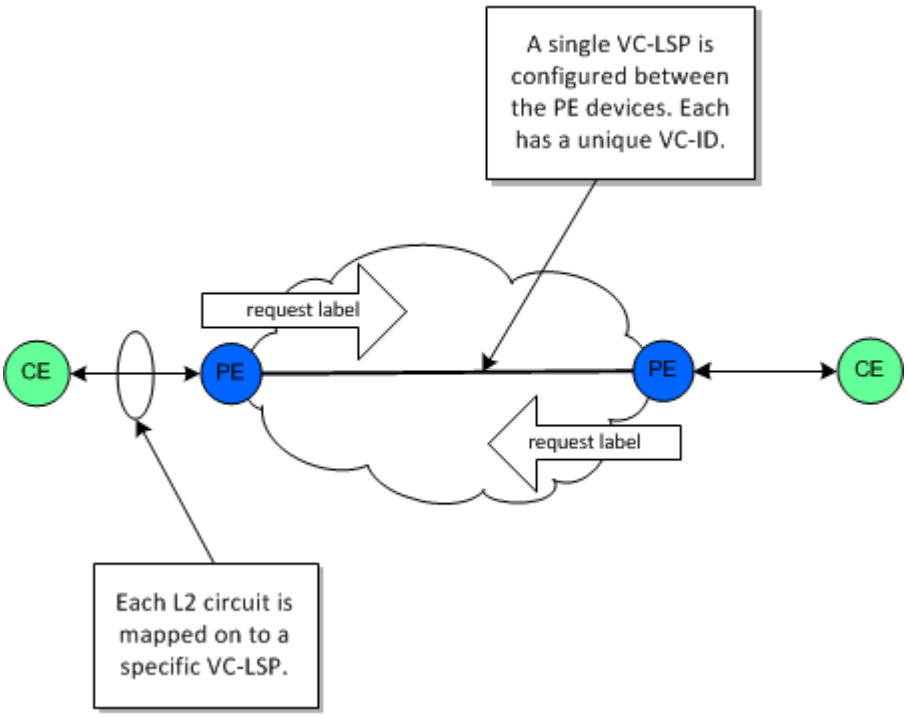
Similarly, Martini solutions can reduce the rollout costs associated with mobile networks in transition from 2G to 3G. Using pseudo-wire, their 2G connection-oriented networks can traverse their new 3G IP core network. This saves the operational costs of supporting two different networks.

Technical Description of Layer 2 Martini VPNs

The Martini draft, IETF's Pseudo-Wire Emulation Edge-to-Edge (PWE3), describes a mechanism that creates a bidirectional point-to-point connection between two PE routers. This connection is called a Pseudo-Wire or a virtual circuit label-switched path (VC-LSP) and consists of two unidirectional Label Switched Paths (LSPs). For further information, refer to RFC 4905.

Creating a PW, illustrated in Figure 3–1, is a two-step process. The first step requires a label distribution protocol (LDP) targeted-peering relationship to be established between the PE routers. Because routers can only exchange labels with their LDP peers, this step is required so that the typically non-adjacent PE routers can exchange labels.

Figure 3–1 Layer 2 Martini Point-to-Point Links



The second step is to request a label for the Layer 2 connection using an extension to the basic LDP signalling. A Layer 2 Forwarding Equivalence Class (FEC) is included in the label request that describes the circuit being connected together over the MPLS core. The returned label is mapped to the circuit described by the Layer 2 FEC and is pushed on the bottom of the label-stack for each of the frames that traverses the network. The PE at either end of the PW repeats this process of label requesting.

Layer 2 circuit emulation (PWE) over MPLS network supports multiple encapsulation types, such as Ethernet (Port), Ethernet (VLAN), ATM Cell, ATM AAL5, and Frame Relay.

A PW is identified by a combination of its VC ID and a Group ID. The Group ID acts as a VC-LSP grouping mechanism (that is, to identify a virtual interface value). The VC ID identifies the PW within the particular group. The Group ID can be seen to equate to the Layer 2 VPN identifier, though its use depends on the specific implementation.

Each Layer 2 frame or other data unit that arrives at the CE-facing interface of the PE is forwarded across the MPLS network with the label negotiated for the PW used to demultiplex it at the destination PE. Because each PE sent the label in response to the Layer 2 FEC, there is a unique mapping.

In addition to the PW label, there is also a control word added to each incoming frame. This includes control flags and a sequence number, used to maintain the frame sequence in order-sensitive traffic.

The full processing of a frame includes the following steps:

- A frame arrives at the PE; its preamble and Frame Check Sequence (FCS) is removed.
- The control word is added to the front of the frame.
- The PW label is added as the bottom-most label in the stack.
- The PE performs a lookup against the IP address for the destination PE, and a transport label that reaches the destination PE is pushed onto the top of the stack. This may be either an RSVP tunnel or LDP LSP.
- The Transport label is swapped as the frame traverses the network and will be (in most cases) penultimate-hop-popped (removed) before reaching the destination PE.
- The destination PE will use the exposed PW label to determine the PW of the frame and from that determine the egress port—it is likely that this will be a single-step lookup in the label table.
- The control word may be used at this point to check the stream order and other relevant administrative functions.
- The FCS and preamble will be reformed and the frame transmitted on the CE-facing interface.

The exact processing varies according to the Layer 2 traffic type being supported.

About Layer 2 Martini VPN Devices and Data Types

This section gives an overview of the different device types and data encapsulations supported by Oracle Communications IP Service Activator in the configuration of Layer 2 Martini VPNs. It also gives specific details for VPN types in which there are variations from the typical configuration.

Layer 2 Martini VPNs on Routers and MPLS-enabled Switching Devices

IP Service Activator supports the configuration of Layer 2 Martini VPNs on MPLS-enabled switching devices, which encapsulate and transmit a number of different types of data.

These devices can be roughly categorized as either MPLS-enabled switching devices or routers.

MPLS-enabled switching devices support Layer 2 and Layer 3 switching features, MAC learning, and VLAN bridging.

Routers support none of the switching features described above but support standard IP routing between interfaces.

Table 3–1 describes the data types that can be encapsulated on Layer 2 Martini VPNs on MPLS-enabled switching devices.

Table 3–1 Data Types on Layer 2 Martini VPNs on MPLS-enabled Switching Devices

Encapsulated Data	Endpoint	Comments
Ethernet (port)	Ethernet port	Martini VLAN ID header is stripped on the pseudo-wire and re-applied (if required) on the exit interface.
Ethernet (VLAN)	VLAN endpoints	Configured under Ethernet interfaces (not sub-interfaces).

All Layer 2 endpoints (such as DLCIs, VLANs, VPI/VCIs) and their parents (logical and physical interfaces) must have the Access role assigned to them.

For Ethernet (Port) encapsulation on MPLS-enabled switching devices, a main interface is used. Endpoint VLAN IDs must be the same on both sides of the pseudo-wire.

For Ethernet (VLAN) encapsulation on MPLS-enabled switching devices, sub-interfaces are not used as the Layer 2 Martini VPN endpoints. You must create new VLAN endpoints or use existing VLAN endpoints. The endpoint VLAN IDs on both sides of the pseudo-wire must be the same.

Table 3–2 describes the data types that can be encapsulated on Layer 2 Martini VPNs on router equipment.

Table 3–2 Data Types on Layer 2 Martini VPNs on Routers

Encapsulated Data	Endpoint	Comments
Ethernet (Port)	Ethernet interfaces	All VLAN tags are preserved across the connection. Frames that enter the tunnel labeled VLAN *n* leave the tunnel labeled VLAN *n*.
Ethernet (VLAN)	VC identifiers	The VC identifier value represents the VLAN ID. The same VLAN ID must be used at both ends of the connection.
ATM Cell	Sub-interface with VC identifier	n/a
ATM AAL5	Sub-interface with VC identifier	n/a
Frame Relay	Main interface with VC identifier	The VC identifier value attached to the main interface must be created manually.

All Layer 2 endpoints (such as DLCIs, VLANs, VPI/VCIs) and their parents (logical and physical interfaces) must have the Access role assigned to them.

ATM Cell Layer 2 Martini tunnel endpoints must have the same VPI/VCI. ATM AAL5 tunnel endpoints are not required to have the same VPI/VCI.

For Ethernet VLAN on routers, VC identifiers are used to represent the VLAN ID. VC identifiers are configured on Ethernet sub-interfaces and used as the Layer 2 Martini VPN endpoints.

For Frame Relay encapsulation on routers, sub-interfaces are not used as the Layer 2 Martini VPN endpoints. You must manually preconfigure or use existing PVCs (permanent virtual circuits) on the main interface.

Inter-operability Between MPLS-enabled Switching Devices and Routers

For inter-operability between MPLS-enabled switching devices and routers, VLAN mode (which retains the VLAN tag across the Martini VC-LSP) must be selected on the MPLS-enabled switching devices. You must also connect to a VLAN VC identifier with the same VLAN ID.

About Creating Layer 2 Martini VPNs

Creating Layer 2 Martini VPNs involves the following steps:

- Add the Layer 2 Martini connections.

- Set the options in the L2 Martini Pt-Pt property page.
- Assign the endpoints to the new Layer 2 Martini tunnel.

Preconfiguration Tasks for Creating Layer 2 Martini VPNs

Before creating a Layer 2 Martini VPN, perform the following preconfiguration tasks:

- Check capabilities of interfaces, sub-interfaces, or provisioned sub-interfaces on the devices to confirm that they support the endpoints of the Martini tunnel.
- Enable MPLS on all required interfaces.
  - Configure the use of the LDP
  - Enable TDP (tag distribution protocol) tag-switching
- On PE devices, configure an IGP, such as OSPF or EIGRP, in order to distribute IP routes. These are required for IP connectivity and to enable labels to be allocated by the separate LDP or TDP.
- Configure tag-switching of IPv4 packets on the WAN-facing (core-facing) interfaces. (These are not the same interfaces on which sub-interfaces for the Layer 2 Martini VPN tunnel endpoints are to be configured.)
  - Enable tag-switching of IPv4 packets on the specified device or interface.
  - If tag-switching is on the interface (WAN facing interface), it should be configured at the interface context.
- Configure devices used in Layer 2 Martini VPNs to use the Gateway role. Configure interfaces used as endpoints to use the Access role.

For vendor-specific information, refer to the vendor's documentation.

Checking Interface Capabilities

Before creating a Layer 2 Martini VPN, check the capabilities of the interfaces, sub-interfaces, or provisioned sub-interfaces on the devices to determine if they will support the endpoints for the Martini tunnel.

To check the interface capabilities for supporting a Layer 2 Martini VPN:

1. Right-click on the interface and select **Properties**.
2. Display the **Capabilities** property page.
3. Under Outbound Capabilities, expand **Martini**.
4. Ensure that the type of encapsulation you wish to use in your Layer 2 Martini VPN is supported by the interface.
5. Confirm that the role for the interface is set to **Access**.

Manually Preconfiguring Martini Circuits on Ethernet Interfaces

If any physical interface encapsulation incompatibilities pre-exist on the router, IP Service Activator detects them when the device driver or cartridge is building a new configuration for Martini circuits. An error is displayed in the IP Service Activator client, and you are given the option to manually correct the interface encapsulation.

In order to expedite the configuration process, ensure that the following manual configuration exists on the router:

- For 802.1Q VLANs or VLAN-based Layer 2 circuits, or both, ensure that VLAN-tagging is enabled on physical interfaces and that each logical sub-interface has a VLAN ID configured.
- For physical Ethernet interfaces to be used in port-based Martini circuits, ensure that there is no VLAN-tagging and either only unit 0 or none of the logical sub-interfaces is present.

Creating a Layer 2 Martini VPN

In order to create a Layer 2 Martini VPN, you need Layer 2 endpoints.

You can create sub-interfaces manually, through the Configuration Template Module or by using the Interface Configuration Module and cartridges (if available for the vendors of interest). For MPLS-enabled switching devices, you can also use the VLAN configuration policy and cartridge (if available for the vendors of interest) to configure VLAN endpoints. For information about configuration policies, see *IP Service Activator QoS User's Guide*.

You must provision the Layer 2 endpoints with the correct encapsulation for the type of Layer 2 Martini VPN you are creating. You can then create the Layer 2 Martini VPN object, set the options, and assign the relevant endpoints to the VPN.

For an overview of prerequisite tasks, see "Preconfiguration Tasks for Creating Layer 2 Martini VPNs".

To create a Layer 2 Martini VPN:

1. In the Hierarchy pane, click the **Service** tab.
2. Click the **Customers** folder.
3. From the displayed customers list, select the required customer.
4. Right-click the **Point to Points** folder and select **Add L2 Martini Pt-Pt** from the context menu.

   The L2 Martini Pt-Pt dialog box appears.
5. Select the **L2 Martini Pt-Pt** property page and specify the following values:
   - **Name**: specify a name for the Layer 2 Martini VPN. The name may contain alphanumeric characters only and may not include spaces.
   - **Remarks**: add any additional remarks (optional).
   - **Type**: choose the appropriate encapsulation type, matching the encapsulation selected when you preconfigured the sub-interface endpoints:
     - ATM AAL5
     - ATM Cell
     - Ethernet
     - Ethernet VLAN
     - Frame
   - **Martini VC ID**: if **Automatic** is selected, IP Service Activator provides a VC ID for you. Otherwise, specify a VC ID.
6. Select the Ownership property page and specify the details to restrict access to the Layer 2 Martini VPN object (optional).

7. Add Layer 2 endpoints (interfaces, sub-interfaces, provisioned sub-interfaces or VC interfaces) to the Layer 2 Martin VPN by doing one of the following:

   - Drag the desired Layer 2 endpoint objects into the new Layer 2 Martini VPN object. This selects them as the Layer 2 endpoints.

     or:

   - Use the Layer 2 Site objects, for Ethernet port and Ethernet VLAN encapsulations on MPLS-enabled switching devices, where you specify the VLAN IDs and to which you link the Ethernet port. For information on Layer 2 sites, see "Setting Up Layer 2 Sites" and "Associating a Physical Component with a Layer 2 Site".

8. On the TLS Site page of the Layer2 Site dialog box, select **Martini Service** from the Service Type list.

For details about the L2 Martini Pt-Pt dialog box, see the L2 Martini Properties page in IP Service Activator online Help.

Implementing the Layer 2 Martini VPN

After the Layer 2 Martini point-to-point connection details are set up and the relevant devices are managed, apply the entire configuration by committing the transaction.

When you commit the transaction, the Martini VPN concretes that will be created are listed in the Concretes page of the Transaction dialog box.

Any validation errors are reported in the Fault page of the Transaction dialog box and the Current Faults pane.

If you wish to cancel the transaction after reviewing the Martini VPNs' concretes that will be created and the faults generated by the transaction, click **Cancel**.

If you wish to proceed with the transaction, click **OK**. Configuration details are sent to the proxy agent/network processor and on to the appropriate device driver/cartridge.

Viewing Implemented Layer 2 Martini VPNs

You can view a list of the Martini VPNs that have been propagated to the network and installed on an interface or sub-interface.

To view implemented Martini VPN details:

1. In the Hierarchy pane, click the **Service** tab.
2. Click the **Customers** folder.
3. From the displayed customer list, select the required customer.
4. Click the **Point to Points** folder.

   The list of implemented Martini VPNs is displayed.

5. Double-click the required Martini VPN.

   The Details pane for that Martini VPN is displayed on the right.

6. Click the **Pt to Pt connections** tab to view the Martini VPNs that are implemented on the selected object. All Martini VPNs' concretes appear on a yellow background.

   Martini VPN details are listed under the following headings:

   - **Point to Point**: The name of the point-to-point Martini VPN

- **Interface Name**: The interface associated with the Martini VPN
- **State**: The current state of the Martini VPN:
  - **Inactive**: The Martini VPN has been created but has not been propagated to the proxy agents
  - **Active**: The Martini VPN has been propagated to the proxy agents
  - **Rejected**: The Martini VPN configuration was rejected
  - **Installed**: The Martini VPN configuration has been installed on the designated interface
- **Conflict** There is a configuration error in the Martini VPN
- **ID**: The internal ID number by which the Martini VPN is identified

4

Setting Up Dedicated Internet Access Services

This chapter describes a method for configuring Dedicated Internet Access (DIA) Services through simple Layer 3 interface configuration and Internet access routing. It includes the following:

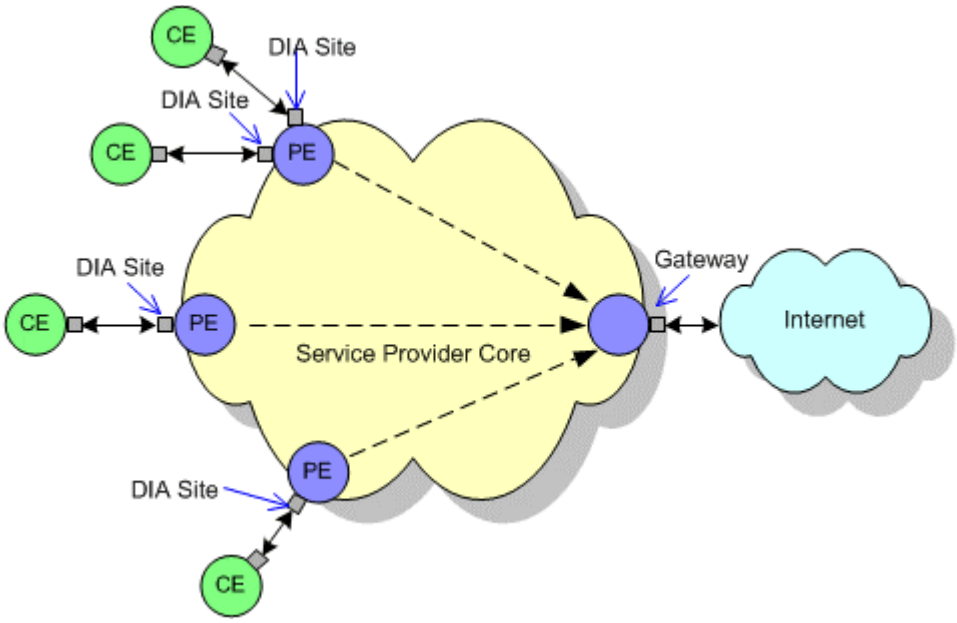
> **Note:** Many service providers use Layer 3 MPLS VPNs as a technology to enable Dedicated Internet Access Services. For more information, see "Setting Up MPLS VPNs". Other technologies can also be used, such as pseudo-wire Layer 2 MPLS Martini VPN. For more information, see "Setting Up Layer 2 Martini VPNs".

About DIA Services in IP Service Activator

Oracle Communications IP Service Activator supports DIA Services through a combination of capabilities built into the IP Service Activator service model and the application of interface and routing configuration policies. This is done through the configuration of Layer 3 interfaces on the PE and the configuration of basic routing (typically static routes) to provide reachability to Internet gateways.

Figure 4–1 illustrates a typical scenario in which it is required that each customer site be able to access the Internet. This is accomplished through the use of DIA sites on the connected PEs.

Figure 4–1 DIA Sites Providing Internet Access



A Layer 3 interface is configured or created and placed in a DIA site. In a managed CE service, the CE device is also placed in the DIA site. IP routing is configured on the PE to route Internet traffic across the provider core to the Internet gateway and on to the Internet. Additionally, prefix lists may be configured to filter routing updates.

Each DIA site represents a physical location and includes an access interface on a PE device, and a CE device. It is used to link the CE device to the PE interface so that routing to the Internet gateway can be provided.

For each of these DIA sites, you need to create a logical Layer 3 interface on the PE dedicated to that site. Each Layer 3 interface will have a different IP address (because they are public IP addresses), and will connect to the service provider public network routing.

In IP Service Activator, site object parameters (such as routing) are only usable within the context of a Layer 3 VPN. For a DIA site, these parameters will therefore not be used. DIA routing is applied through routing configuration policies or templates.

Note: You can include the CE device under the DIA site and manage it in the context of a managed-CE service, so that you can supply additional configuration such as QoS mechanisms.

About Configuring DIA Services

Configuring DIA services for a customer site involves the following steps:

- Creating a DIA Site Folder
- Configuring or Creating a PE Layer 3 Interface
- Creating a DIA Site Under the DIA Site Folder
- Linking the PE Layer 3 Interface to the DIA Site
- Configuring Internet Access Routing for the DIA Site
- Linking the CE Device to the DIA Site

After you complete these steps, you can optionally provision other services such as QoS on the CE device, and on the PE Layer 3 interface.

The procedures given to configure DIA services assume a certain level of vendor cartridge support, such as for creating an interface, configuring routing and so on. Refer to the appropriate vendor cartridge guides to confirm which configuration policy capabilities are supported for each vendor equipment family. Cartridge extensions can be created using the IP Service Activator Software Development Kit (SDK).

Note: You can choose to commit transactions at various stages of the DIA configuration, or leave the commit until the end, to reduce impact on the system.

Creating a DIA Site Folder

A DIA site folder must be created under the Customers folder in IP Service Activator for each customer which has CE devices to be connected to the Internet. This folder can contain multiple DIA sites.

To create a DIA site folder:

1. In the Hierarchy pane, click the **Service** tab.
2. Expand the **Customers** folder.
3. From the displayed customers list, select the required customer.
4. Right-click the Sites folder and select **Add Folder** from the context menu.
5. Specify a name for the folder (for example, DIA).
6. Click **OK**.
7. Commit the transaction.

   The DIA site folder is created.

Configuring or Creating a PE Layer 3 Interface

A PE Layer 3 interface is required to be linked to the DIA site. This interface can be an existing physical interface, an existing sub-interface, or a sub-interface which is created using IP Service Activator.

To create a PE Layer 3 interface from a new sub-interface:

1. Create Interface Policy Registrations. For information, see *IP Service Activator QoS User's Guide*.
2. Install the appropriate policies. For information, see *IP Service Activator Installation Guide*.
3. Create a sub-interface using either the interface management configuration policies, or a configuration template (through the Configuration Template Module). For details, see *IP Service Activator QoS User's Guide* and the IP Service Activator online Help.

Whether you use an existing interface or sub-interface, or create a sub-interface, you must specify the settings required for your configuration, including interface parameters, the interface role, and an IP address.

You would typically give the PE device a role of Gateway, and the PE Layer 3 interface a role of Access. For example, when configuration policies are applied to configure static routing, the roles can be specified for the configuration policy so that it is applied to the correct interface.

Creating a DIA Site Under the DIA Site Folder

After creating the DIA site folder, you need to create a DIA site under it. For information on DIA site folder, see "Creating a DIA Site Folder".

To create a DIA site under a DIA site folder:

1. Right-click the DIA site folder that you created in "Creating a DIA Site Folder" and select **Add VPN Site** from the context menu.
2. Specify a name (for example, “DIA Site”).
3. Click **OK**.
4. Optionally, commit the transaction.

   The DIA site is created.

Linking the PE Layer 3 Interface to the DIA Site

To link the PE Layer 3 interface to the DIA site:

1. Click the **Topology** tab.
2. In the Details pane, double-click the PE device to display its interface.
3. Click the **Service** tab.
4. Navigate to the DIA site folder.
5. Drag the PE Layer 3 interface to the DIA site.
6. Optionally, commit the transaction.

Configuring Internet Access Routing for the DIA Site

After the PE Layer 3 interface and the DIA site have been linked, you must configure routing so that traffic can reach the Internet access gateway (or gateways) from the DIA site.

One way to accomplish this is to set up appropriate static routes to direct traffic destined for the Internet through the IP address of the Internet gateway. Static routes can be configured by applying the Static Route configuration policy on the site.

Use roles to control the application of configuration policies. For example, set the device role to Gateway and the PE Layer 3 interface role to Access. Set a matching role on the configuration policy so that it is applied to the PE Layer 3 interface.

To apply a static route to the PE interface:

1. Click the **Service** tab and navigate to the DIA site.
2. Right-click the PE interface, select **Add Configuration Policy**, select **General**, and then select **Static Route**.

   The Configuration Policy dialog box appears.
3. In the Name field, provide a name.

4. Select either **Add IPv4 Static Route** or **Add IPv6 Static Route**:
   - If you select **Add IPv4 Static Route**, specify the values including **Destination Prefix**, **Destination Mask**, **Next Hop IP**, **Exit Interface Name**, and **Distance Metric**.
   - If you select **Add IPV6 Static Route**, specify the values including **Destination Prefix/Length**, **Next Hop IP**, **Exit Interface Name** and **Distance Metric**.

   You can define multiple IPV4 and IPV6 static routes within a single Static Route configuration policy.
5. Specify an appropriate role so that the configuration policy is applied to the correct interface.
6. Click **OK**.
7. Optionally, commit the transaction.

For details on the fields in the Static Route configuration policy, see the IP Service Activator Online Help.

Linking the CE Device to the DIA Site

The CE device must be linked to the DIA site so the site can access the device.

To link the CE device to the DIA site:

1. Click the **Topology** tab.
2. In the Details pane, double-click the parent folder of the CE device.
3. Click the **Service** tab.
4. Navigate to the DIA site folder.
5. Drag the CE to the DIA site.
6. Optionally, commit the transaction.

5

VLAN Configuration in Metro Ethernets

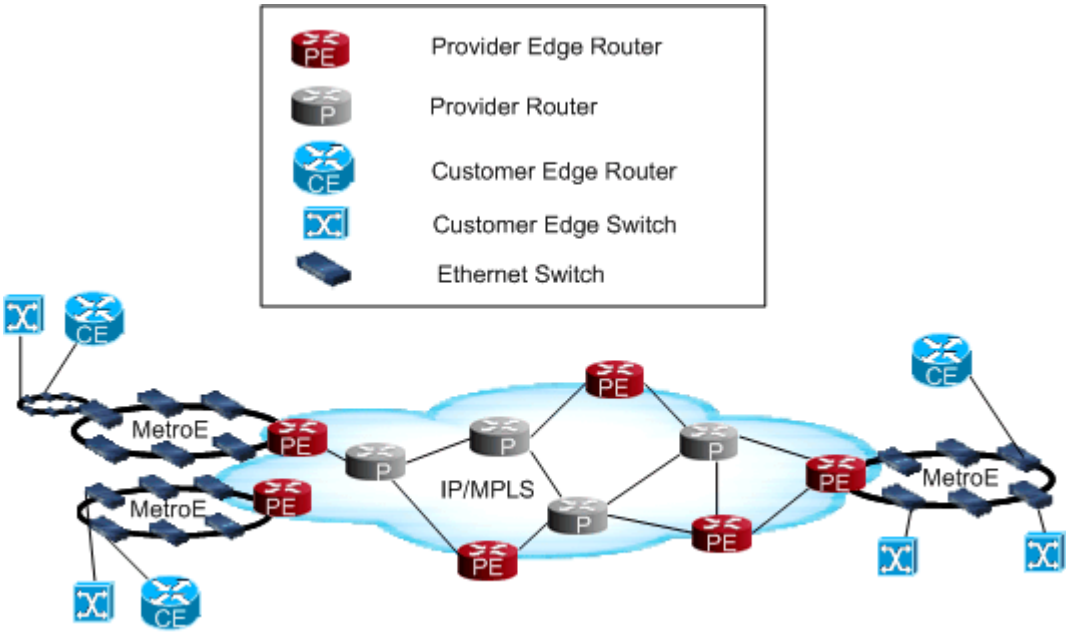
This chapter explains how to configure VLANs using Oracle Communications IP Service Activator.

About VLAN Configuration in Metro Ethernets

This chapter describes VLANs in terms of a typical large service provider scenario. The service provider has a large IP/MPLS core network with a wide geographic reach. This core network can be nationwide or even global in scope. In various cities, the evolution is to use Metro Ethernets to connect many customers to the local, large Provider Edge (PE) device. Sometimes when a customer is close enough to the core network, a Customer Edge (CE) device can connect directly to the PE without the use of a Metro Ethernet.

Figure 5–1 illustrates the configuration of VLAN in a Metro Ethernet network.

Figure 5–1 VLAN Configuration in Metro Ethernet Network



Depending on physical distance, a Metro Ethernet network may be small or large. A small Metro Ethernet network can be a single switch (or two for redundancy if placed in parallel), each connected to their own PE interface on a PE router.

Metro Ethernet network can have 30, 40, 50, or more switches in it depending on the number of customers. Where multiple customers connected to the same Metro Ethernet network, need to configure separate VLANs on the Metro Ethernet network to provide transport from the Metro Ethernet network to the IP/MPLS core.

Metro Ethernet Topologies

Metro Ethernet can be organized in four types of topologies:

- Line Topology
- Full Mesh Topology
- Partial Mesh Topology
- Ring Topology

Line Topology

An example of a line topology is two switches in a sequence:

CE—Switch—Switch—PE

This topology is not redundant. If either of the switches goes out, the connection to the PE is broken.

Full Mesh Topology

An example of a full mesh topology is six switches physically connected to each other. The advantage is if one link goes down the traffic can take another path.

Partial Mesh Topology

This is the most common topology. Few switches feature multiple connections to other switches, but not all switches are fully interconnected as in full mesh topology.

Ring Topology

Figure 5–1, "VLAN Configuration in Metro Ethernet Network" illustrates ring topology. This topology is more efficient for provisioning and maintaining because of fewer connections than a mesh topology. The advantage is if one device fails, traffic can go through the other side of the ring.

In a large service provider scenario, a Metro Ethernet ring can connect to one or more smaller, secondary Metro Ethernet rings to further extend the geographic stretch (or reachability) to remote customers.

This topology can have a single link to a single switch for the secondary ring to reach smaller customers.

Example of Configuring VLANs on Metro Ethernets

In a large service provider scenario, VLAN provisioning occurs in the Metro Ethernet network and at access points from the PE to the Metro Ethernet network. If you want to connect the CE on the second ring at the upper-left to a Layer 3 VPN on the PE, there are a number of connections involved, especially between the twelve switches. The PE is attached to the Metro Ethernet ring through two Ethernet switches, one on each side of the ring.

PE Connections and Configuration

The PE requires a Layer 3 VPN site which includes two different access interfaces. These interfaces are Ethernet VLAN sub-interfaces. They are Layer 3 sub-interfaces created on the PE device using the interface policy registration in IP Service Activator. The VLAN sub-interfaces are associated with a particular VLAN ID (for example, VLAN ID 5) using the following command:

```
encapsulation dot1q
```

For information on the configuration policy used to create sub-interfaces, see the IP Service Activator Online help.

For information on interface policy registration, see "Registering Interface Policies and Creating Interfaces".

A Metro Ethernet network can support multiple VLANs and multiple customers. At the PE, all VLAN traffic from the Metro Ethernet network can arrive at the same PE port. However, the PE port is configured with separate VLAN sub-interfaces, one to match each VLAN configured on the Metro Ethernet network. The traffic tagged with a particular VLAN ID is routed to the PE through the matching VLAN sub-interface.

Metro Ethernet Configuration

Continuing the example from above, the Metro Ethernet network is configured to support VLAN ID 5, so as to know where to send traffic tagged with that VLAN ID.

All devices in the primary and secondary ring must be configured to support VLAN ID 5. All interconnections between the Ethernet switches (that is, trunk ports), as well as, the switch to PE router connections have to be enabled for VLAN ID 5. This allows traffic tagged with VLAN ID 5 to be sent across the trunk ports. Each of these configurations requires a separate manual step.

In order to perform the needed configurations, you must log in to all the twelve switches on the left ring, create VLAN ID 5 on all 12, and configure 26 trunk ports (two per device including one device with four trunk ports).

To perform this configuration manually is very demanding and error prone. If any one of the trunk ports on the two Metro Ethernet rings is not enabled or misconfigured, the ring is broken and there will be only one path remaining to go through. If a second trunk port is misconfigured, connectivity between the CE and PE (and IP/MPLS core) is broken.

Configuring CE Access

The CE is connected to a switch on the Metro Ethernet ring through a port which also needs to be configured as either an access or trunk port. The VLAN configuration is applied so that all Ethernet frames are tagged with VLAN ID 5. Then the frames are broadcast across the Metro Ethernet network.

At this stage, everything is configured so that frames can travel from the CE, across the Metro Ethernet networks, to the PE, onto the VPN, across IP/MPLS core, to the destination Metro Ethernet network, onto the access device (CE) and finally to the receiver.

VLAN ID is local to the Metro Ethernet rings and is dropped when the traffic passes onto the IP/MPLS core. The Metro Ethernet network that the destination CE is connected to could use a different VLAN ID.

The Metro Ethernet network can support many different customers each with their own VLAN ID, so that there is no visibility of traffic between customers. For example, a Metro Ethernet ring could be provisioned with 200 different VLAN IDs.

At the PE, multiple VLAN IDs can arrive into the same port, but with different VLAN sub-interfaces, each associated with their respective Layer 3 VPN.

This configuration exercise can be extremely time consuming and error prone involving thousands of decision points.

Configuring VLANs with IP Service Activator

This section explains how IP Service Activator implements VLANs.

About Configuring VLANs with IP Service Activator

VLANs are configured on Metro Ethernet networks in IP Service Activator using a policy-based approach. A network object is created in IP Service Activator to represent the Metro Ethernet network. All devices in the Metro Ethernet network would be included under the network object. An appropriate custom role is applied to these devices and to the interfaces which are trunk port connections within the VLAN.

One configuration policy is used to define the VLAN IDs on the Metro Ethernet network and a second is used to apply trunk port configuration to the appropriate interfaces. The configuration policies are applied at the network level and role-based inheritance ensures that the configuration is distributed to the appropriate devices and interfaces, and applied as device configuration commands by IP Service Activator.

This powerful policy-based approach greatly reduces potential configuration errors and makes maintenance of the VLAN configuration easy.

Another advantage is that as additional devices are added to the Metro Ethernet network, you need to only discover them and apply appropriate device and interface roles, and all the required VLAN configuration is automatically applied. In case, you need to remove or add support for a single VLAN ID, the change is made in one place (on the vlanDefinitions configuration policy) and is automatically updated throughout your network.

Using Configuration Policies to Manage VLANs in IP Service Activator

Table 5–1 shows the topology points that must be configured between the CE and PE, and the Metro Ethernet between them to support a VLAN.

Table 5–1 Topology Points Required to Support a VLAN

Topology Points	Required Configuration
On the PE	PE interface and access port
On the access switch connected to the PE	Trunk port
On the Metro Ethernet switches	Trunk port
On the access switch connected to the CE	Access port and trunk port

The vlanDefinitions configuration policy can be used to define VLANs at the network level. The vlanDefinitions configuration policy is applied on the PE interface. By setting roles on target devices and interfaces, inheritance is used to apply the VLAN configuration to the appropriate devices and interfaces. The vlanDefinitions configuration policy can be used to define up to 200 VLAN IDs.

The vlanInterface configuration policy is applied to the switch ports and access ports connecting to the PE and CE.

The device level configuration policy should be applied to a Loopback interface. For more information, see *IP Service Activator QoS User's Guide*.

The vlanInterface configuration policy can be applied at the network level. By setting roles on target devices and interfaces, inheritance is used to apply the configuration policy to the appropriate devices and interfaces.

Separate instances of the vlanInterface configuration policy are used to configure access ports and trunk ports. It is important to ensure that separate roles are used to distinguish the two types of policy targets. One instance of vlanInterface configuration policy is applied to each customer site access port. Only one VLAN ID is allowed to be specified on this port.

Discovery and Role Assignment for VLAN Configuration

When you discover the devices and switches that will be configured to support VLAN, ensure you create a structure within the IP Service Activator object model hierarchy that will reflect your strategy for grouping targets so that policy inheritance will flow correctly.

Within a Metro Ethernet network, consider creating a custom role that applies to the network and the devices under that network that make up the Metro Ethernet network. Using this role, the vlanDefinitions configuration policy can be automatically applied to all devices in the Metro Ethernet network that require VLAN configuration, because it will be inherited by all devices with custom role.

Where there are primary and secondary Metro Ethernet rings, you may require different custom roles so that you can address each Metro Ethernet network separately, for management purposes.

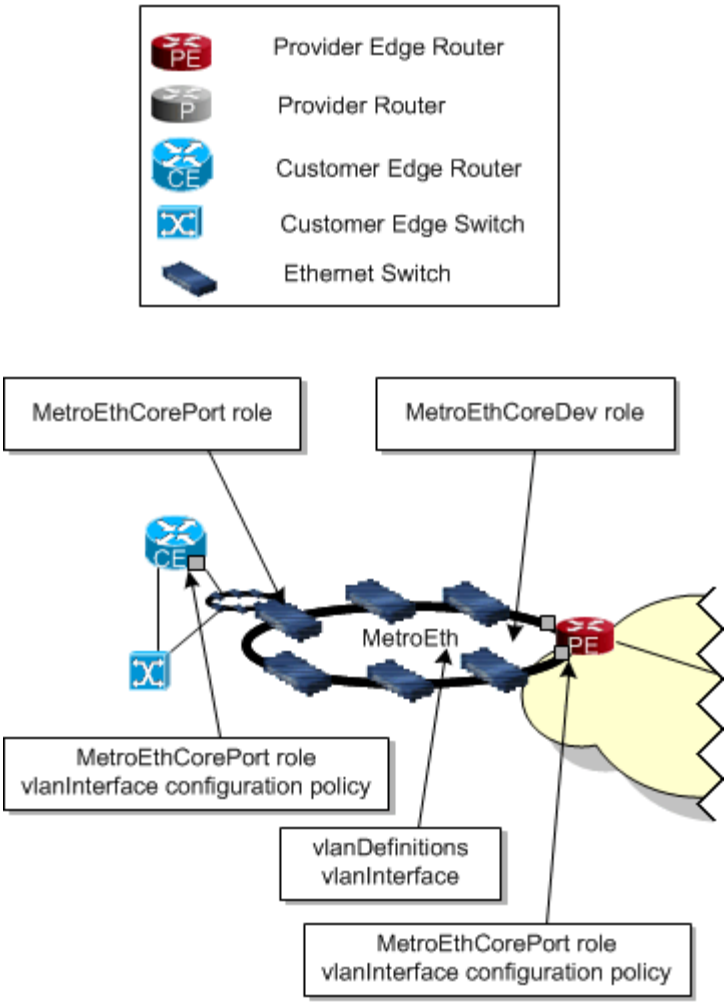
As additional devices are added to a Metro Ethernet ring, they can be discovered into the appropriate IP Service Activator network and given required roles.

Example of VLAN Role Assignment

Consider a single Metro Ethernet ring.

Figure 5–2 illustrates the application of VLAN role and configuration policies.

Figure 5–2 Application of VLAN Role and Configuration Policies



To assign VLAN roles and configuration policies as in Figure 5–2:

1. In the IP Service Activator client, take the devices that are in the Metro Ethernet network and group them into the same network (for example, **MetroEth**).
2. Create a custom role called **MetroEthCoreDev** to identify devices that are included in the MetroEth network.

   For information on creating a role, see *IP Service Activator User's Guide*.
3. Apply the MetroEthCoreDev role to all devices in the MetroEth network.
4. Create another custom role called **MetroEthCorePort** to identify trunk ports.
5. Apply the MetroEthCorePort role to each trunk port.
6. Apply the vlanDefinitions configuration policy to the MetroEth network and apply the role MetroEthCoreDev.

   All devices in the network will receive the VLAN configuration specified by the vlanDefinitions configuration policy.
7. Apply the vlanInterface configuration policy to the MetroEth network and apply the role MetroEthCorePort.

All trunk ports in the network will receive the VLAN interface configuration specified by the vlanInterface configuration policy.

8. The CE access port must be configured either as a trunk port or an access port as follows:
   - If configured as a trunk port, the MetroEthCorePort role is applied to the interface, which will cause the vlanInterface configuration policy to be applied. In this case, traffic travelling out of this port onto the Metro Ethernet network is tagged with a VLAN ID.
   - If configured as an access port, the port can handle traffic destined for multiple VLAN IDs. The traffic traveling out of this port onto the Metro Ethernet network is not tagged with a VLAN ID—this happens on the device in the Metro Ethernet network to which it is connected.
9. Configure the port on the PE which connects to the Metro Ethernet network as either an access or trunk port similar to CE access port configuration.

Configuring the VLAN Using Configuration Policies

The following two configuration policies are provided with IP Service Activator for configuration of VLAN.

- **vlanDefinitions**: Allows you to create VLAN definitions on devices. Various parameters including the VLAN ID and name can be specified. Up to 200 VLAN IDs can be specified in a single instance of this policy. Multiple instances of the vlanDefinitions configuration policy can be applied on the device to configure more VLANs.
- **vlanInterface**: Allows you to configure a VLAN on an interface. Multiple VLAN IDs can be specified in a single instance of this policy. Alternatively, multiple instances of the vlanInterface configuration policy can be applied to an interface to configure more VLANs.

For details about the fields provided in these configuration policies, see IP Service Activator online Help.

Balancing Manual and Policy-based VLAN Configuration

In some cases there may be a requirement to trade-off between redundancy and resiliency, and speed within a Metro Ethernet network.

For example, a partial mesh Metro Ethernet network with fewer VLAN IDs configured on it may switch faster due to less broadcasting of VLAN tagged packets across the network, but provide less redundancy. A full mesh Metro Ethernet network with a lot of VLAN IDs managed by a configuration policy applied across the network is easier to maintain in terms of operator actions, and provides high resiliency, but might switch packets slowly across the network due to a higher hop count.

Consider an efficient VLAN configuration set up with individual configuration policies applied to all involved target objects (interfaces and devices) on the Metro Ethernet network. This VLAN configuration will be very labor-intensive, slow to provision and maintain, and error-prone.

Instead, if you choose to accept more Ethernet broadcasting, you can have a VLAN configuration in which you can provision services very quickly using a full or partial policy-based approach.

Oracle can provide consulting to help you achieve an optimal solution to match your requirements.

Table 5–2 illustrates various trade-offs that can be considered for your VLAN configuration.

Table 5–2 VLAN Configuration Trade-offs

Topology	Fiber Efficiency	Hop Count	Resilience
Spur	Low	1	None
String	Medium	High	None
Tree	High	High	None
Meshed	High	High	Full or partial
Ring	High	High	Full, fast

6

Setting Up Transparent LAN Services

This chapter describes how to configure Transparent LAN Services (TLS) and transparent VLAN services.

Note: Multiple Transparent LAN Service technologies exist, such as MPLS-based VPLS and Ethernet switching-based VLANs. Only VPLS is implemented in Oracle Communications IP Service Activator.

About VPLS Service

A VPLS connects separate customer Ethernet LAN segments through an MPLS network. The connection across the network appears to the customer as a single LAN segment.

IP Service Activator supports the encapsulation and transport of layer 2 frames across the VPLS as described in the Lasserre TLS Draft.

Configuration of the VPLS occurs at Provider Edge (PE) devices within an MPLS network. Ethernet frames are mapped to a particular service instance based on a combination of the port on which they arrive at the PE device and, optionally, the 802.1Q tag that has been applied to them. As with other VPN solutions, inner and outer tunnels are used:

Outer tunnels provide a transport mechanism between the PE routers in the VPLS

Inner tunnels, referred to as VC-LSPs, form a full mesh between the PEs in each VPLS instance and are particular to that VPLS.

Multiple VC-LSPs may be carried by a single transport ‘outer’ LSP.

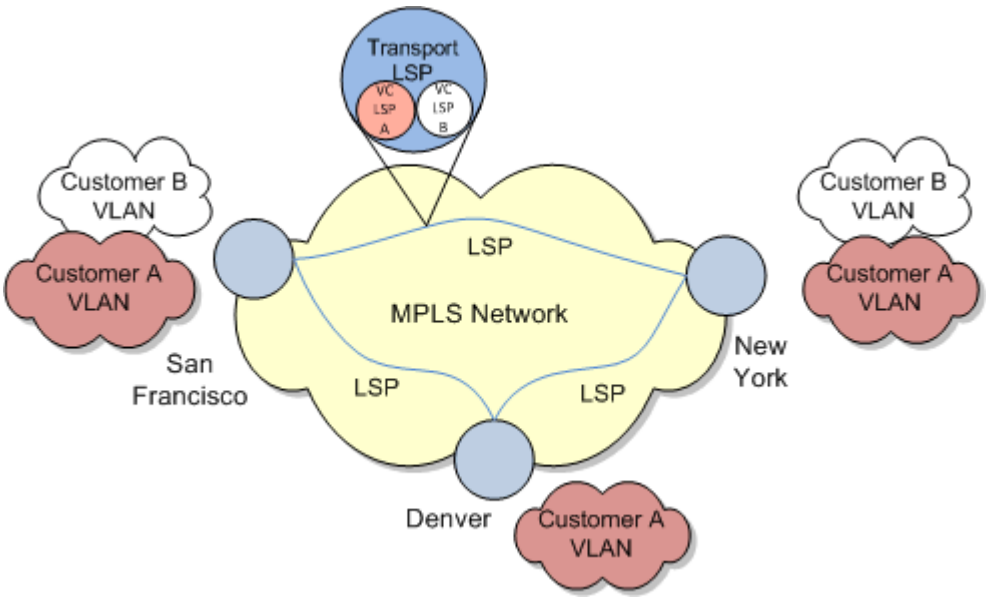
About VC-LSPs

The Lasserre VPLS solution uses VC-LSPs as defined in the Layer 2 Martini over MPLS Internet drafts. A targeted LDP peering association between two PE devices creates the VC-LSP. The devices exchange information about the Layer 2 protocol that will be carried. In the TLS case, this is either untagged or 802.1Q tagged frames. This exchange also includes information about the VPLS instance of which the VC-LSP forms a part. The Forwarding Equivalence Class (FEC) thus describes Layer 2 information, rather than the more usual IP prefix.

Each PE sends back a VC-LSP label, which is mapped to the FEC. When a frame is received at the PE, it examines its forwarding table and applies the correct VC-LSP label. The correct transport label is then added and the frame is forwarded to the correct destination. At the egress PE router, the VC-LSP label is used to identify the correct Ethernet port over which to forward the enclosed frame.

In Figure 6–1, VC-LSPs are configured for the Customer A VPLS instance between San Francisco, Denver and New York. The VC-LSPs are contained within the transport LSPs that connect these destinations.

Figure 6–1 VC-LSP Configuration



Transport LSPs

Transport LSPs are responsible for linking PE routers together. Each VC-LSP must be forwarded to the correct PE by the transport LSP.

802.1Q Support

The IEEE standard 802.1Q describes a VLAN tag that can be applied to an Ethernet frame. The tag value is the VLAN ID, a number assigned to switches in an Ethernet network. Tagged frames can only be forwarded to switches that are configured with the same VLAN ID as the tag. Switches may be in more than one VLAN at a time, connected by trunk ports over which tagged frames are sent. Access ports to the Ethernet network may only be assigned a single VLAN ID. The frames arriving at an access port are untagged.

Mapping Frames to the VPLS

To complete the VPLS service, a mapping must be established between incoming Ethernet frames to the PE and the VC-LSPs that are configured over the MPLS core. This mapping can be:

- Port based: all frames from a particular port are mapped to the service.
- VLAN based: all frames with an 802.1Q tag of a given value are mapped to the service.
- "Port and VLAN" based: all frames from a particular port with a given 802.1Q tag are mapped to the service.

IP Service Activator supports port-based, and "port and VLAN"-based TLSs. The mapping to the VPLS instance is configured on the PE device.

Ethernet is a broadcast service and this must be replicated in the VPLS. Therefore, when a frame is received at a PE device for an unknown destination, it is forwarded over all the VC-LSPs in the VPLS. When a response to this frame is received at the PE device, the device first learns which VC-LSP the frames were returned over before forwarding the frame over the correct Ethernet port. Future frames to that destination are then only sent over the learned VC-LSP. This mechanism is called 'flood and prune'.

A port that handles incoming traffic to the VPLS may therefore receive tagged or untagged frames and tagged frames may belong to one or more VLANs. Ingress ports to the TLS may be configured as one of the following, depending on whether tagged or untagged frames are handled:

- A **trunk port** receives and transmits tagged frames belonging to one or more VLANs; a trunk port may also be configured to transmit untagged frames by making it part of the native VLAN (typically VLAN 1), but this is not supported by IP Service Activator.
- An **access port** receives and transmits untagged frames and frames belonging to a maximum of one VLAN. By default, access ports are considered to be part of the native VLAN (typically VLAN 1) unless they are explicitly assigned to another VLAN.

Planning a TLS

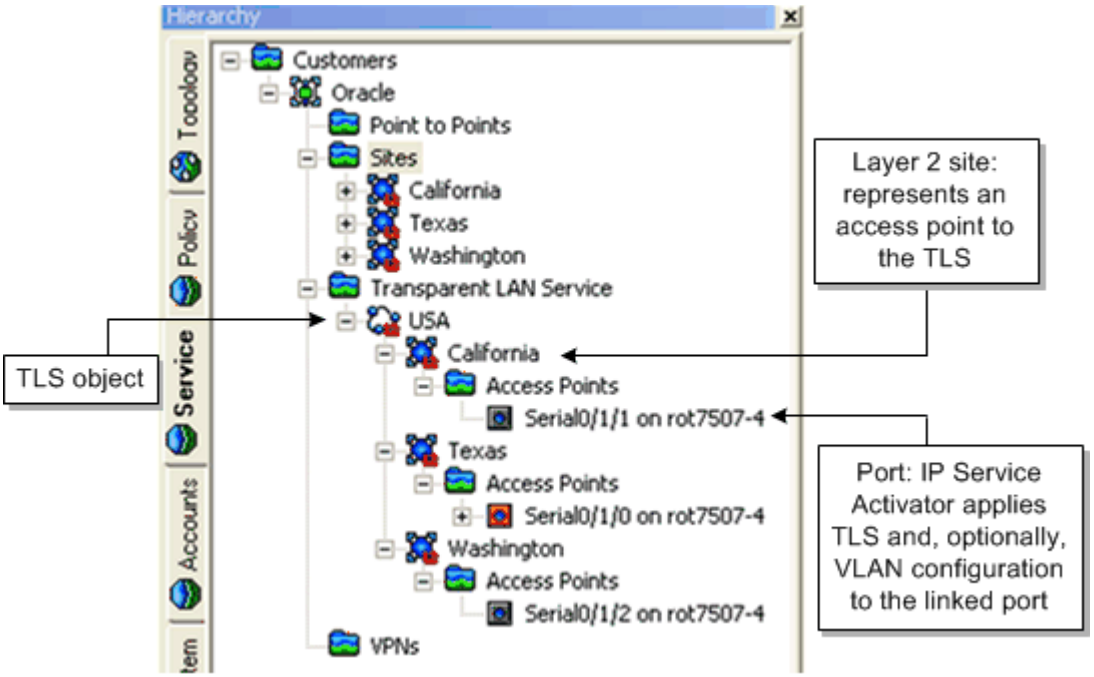
IP Service Activator supports the following TLS types:

- **Port-based**: access to the TLS is controlled by incoming port number
- **"Port and VLAN"-based**: access to the TLS is controlled by incoming port number and VLAN ID.

A TLS is represented by a TLS object in the client, and the edge points of the TLS are represented by layer 2 site objects. Each layer 2 site is linked to one or more ports that indicate where IP Service Activator will apply TLS configuration.

Figure 6–2 illustrates how a TLS is represented in the Hierarchy pane.

Figure 6–2 TLS Hierarchy Representation



IP Service Activator represents a layer 2 port as an interface object in the client. In the descriptions that follow, the term 'interface' is used when referring to TLS setup through the client.

IP Service Activator applies the concept of port and "port and VLAN"-based entry criteria both to the TLS object and the layer 2 sites that are linked to it:

- A port-based TLS consists of a number of port-based layer 2 sites
- A "port and VLAN"-based TLS consists of a number of "port and VLAN"-based layer 2 sites

Creating a TLS

To create a TLS:

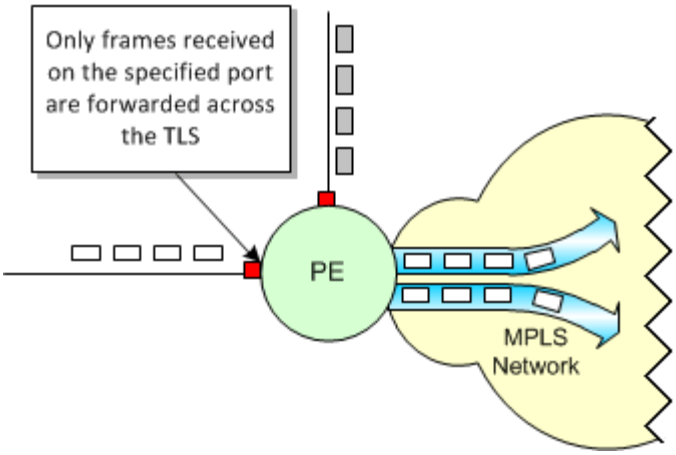
1. Discover the network and assign the correct roles to the devices and ports that you want to participate in the TLS.
2. Create a TLS object. See "Creating a TLS".
3. Create layer 2 sites that represent the edge points of the TLS and link the relevant ports to the sites. See "Setting Up Layer 2 Sites".
4. Link the layer 2 sites to the TLS object. See "Linking Sites to a TLS".

When you link layer 2 sites to a TLS and if the service type is **VPLS Service**, IP Service Activator configures a full mesh of LSPs between peer PE devices.

Port-based TLS

In a port-based TLS, forwarding of frames across the TLS is based on incoming port number, as illustrated in Figure 6–3.

Figure 6–3 Forwarding of Frames Across the TLS



Incoming frames may be tagged frames or untagged frames.

In a port-based TLS, VLAN configuration and management are performed by the service provider and/or its customer. IP Service Activator simply configures the specified ports at the edge of the TLS to be either Ethernet access ports or 802.1Q trunk ports, depending on whether untagged or tagged frames are transmitted across the TLS.

> **Note:** You cannot perform tagging of incoming frames at a port-based site.

You specify whether the TLS accepts tagged or untagged frames when creating the TLS object.

To create a port-based VPLS service:

1. In the TLS Type list, select **VPLS Service**.
2. Select the **Port based (Untagged)** option.

> **Note:** Multiple Transparent LAN Service technologies exist, such as MPLS-enabled VPLS and Ethernet switching-based VLANs. Only VPLS is implemented in the current IP Service Activator version.

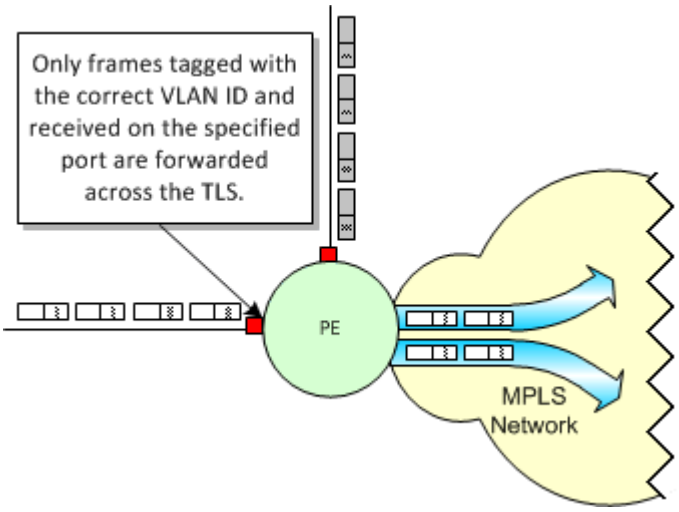
The edge points for the TLS are defined by port-based layer 2 sites. Each site may contain a single port. A port-based site may be linked to one port-based TLS.

You specify on which ports incoming frames for the TLS will be received by linking the Access interface on the appropriate Gateway (PE) device to a layer 2 site. An interface can be linked to one port-based layer 2 site.

Port and VLAN-based TLS

In a "port and VLAN"-based TLS, frame forwarding is based on incoming port number and the ID of the VLAN to which the frame belongs, as illustrated in Figure 6–4.

Figure 6–4 VPLS Service with Two Ports

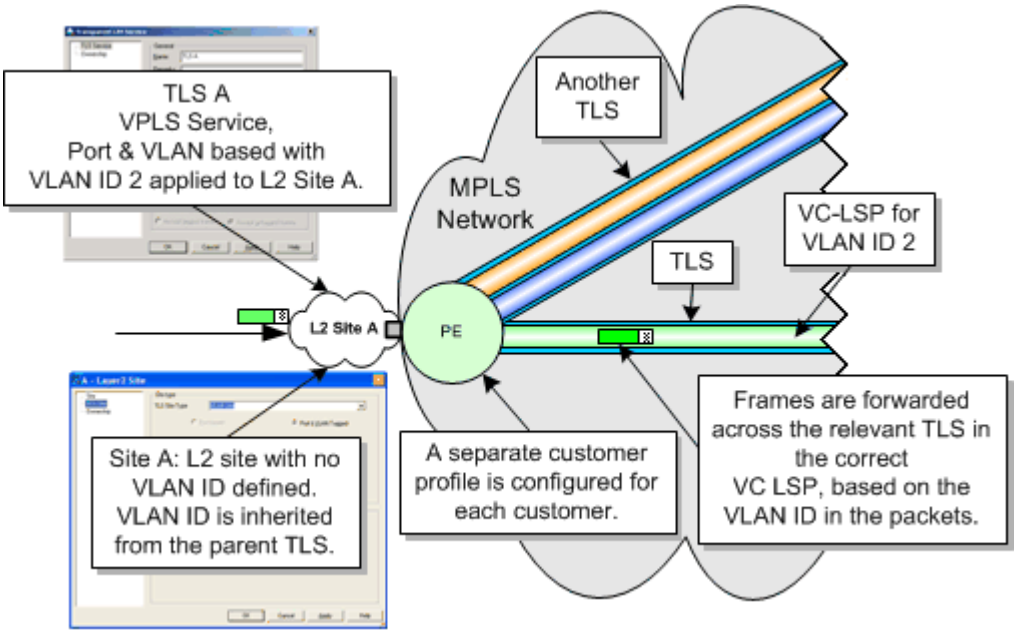


Incoming frames may have been tagged before reaching the entry point to the TLS.

You may also choose not to specify a VLAN ID in the layer 2 site definition. If no VLAN ID is specified for a layer 2 site, the VLAN ID specified for the TLS is inherited to the site.

A layer 2 site that has no VLAN specified in its definition may be linked to a "port and VLAN"-based TLS object. The site inherits the VLAN ID specified for the corresponding TLS. Frames are transmitted across the correct TLS/VC LSP, as illustrated by Figure 6–5.

Figure 6–5 Inheritance of VLAN ID from TLS



At minimum, a layer 2 site may contain a single port – represented by an Access interface on a Gateway (PE) device in the user interface. IP Service Activator configures the port as:

- An access port if the site receives untagged frames

- A trunk port if the site receives tagged frames

Manual Preconfiguration of a TLS

Some manual preconfiguration is required before setting up a TLS. For detailed information on manual preconfiguration, refer to the documentation for your devices.

Perform the following pre-configuration tasks on your PE and P devices:

- Enable and start MPLS and LDP
- Configure the IGP routing protocol

Setting Up a TLS

You create a TLS in IP Service Activator by creating a TLS object and associating layer 2 sites with the object. The sites that you link to a TLS mark the edge-points of the VLANs that are to be interconnected.

For information on planning a TLS, see "Planning a TLS".

Creating a TLS

When creating a TLS object, you define broad characteristics of the TLS:

- For a port-based TLS, whether the TLS accepts untagged or tagged frames.

  IP Service Activator does not create VLANs or assign VLANs to any ports. It simply configures all ports in the TLS consistently as Trunk or Access ports.
- For a “port and VLAN”-based TLS, specify the VLAN ID that could be inherited by the layer 2 sites.

To create a TLS:

1. On the Service tab, open the relevant customer folder, select the **TLS** folder and right-click to select **Add Transparent LAN Service** from the context menu.

   The Transparent LAN Service dialog box opens.
2. On the TLS Service page, specify the following parameters:
   - **Name**: specify a name for the TLS. The name may contain alphanumeric characters only, and may not include spaces or hyphens.
   - **Remarks**: add any additional remarks (optional).
   - **Level**: a level number from 0 to 7 for the TLS. This parameter is only used if a site is a member of more than one TLS and you are setting up QoS or access control on the TLS:
     - Rules are installed from all TLSs. Rules are installed in TLS level order, where rules from the TLS with the lowest level number are installed first and therefore evaluated first.
     - For PHB groups, up to a maximum of one PHB group is installed from the TLS with the lowest level number.

     If two or more TLSs have the same priority level, a conflict is reported. By default the level is set to **4**.
   - **Service type**: specify the criteria on which access to the TLS is based:
     - **TLS Type**: select VPLS Service

  - **Port based**: forward traffic across the TLS according to incoming port number.
  - **Port & VLAN based, with VLANs**: forward traffic across the TLS according to incoming port number and the specified VLAN ID.
- **VPLS VC ID**: VPLS VC ID creation either auto generated or manually.
  - **Automatic**: Leave the check box selected for auto generation of the VC ID or deselect to specify the VC ID manually in the adjacent text box.

  This check box is available only when VPLS Service is selected for the TLS Type.
- If the Service type is **Port based**, specify the Local network port configuration:
  - **Accept tagged frames**: transport only pre tagged frames on the TLS (trunk port).
  - **Accept untagged frames**: transport only untagged frames on the TLS (access port).

3. If you wish to restrict access to the TLS object, select the **Ownership** property page and specify the details. For information on setting ownership options, see *IP Service Activator User's Guide*.

Setting Up Layer 2 Sites

A layer 2 site defines an access point to a TLS:

- A port-based site may have a single port associated with it and be linked to a single port-based TLS. For more information, see "Port-based TLS".
- A port- and VLAN-based site may have multiple ports on the PE associated with it. For more information, see "Port and VLAN-based TLS".

To set up a layer 2 site:

1. On the Service tab, right-click the Sites folder under the relevant customers folder and select **Add Layer2 Site** from the context menu.

   The Layer2 Site dialog box opens.
2. On the Site page, specify an identifying **Name** for the site, and any additional comments.
3. (Optional) Set up account and contact information, if required.
4. On the Transparent LAN Service page, select the **Service type**:
   - **TLS Site Type**: select VPLS Service
   - **Port based**: create a port-based TLS on the port.
   - **Port & VLAN Tagged**: create a port- and VLAN-based TLS on the port.
5. If the Service type is **Port & VLAN Tagged**, use the Local network port configuration frame to specify how the port handles incoming frames by doing the following:
   - **Accept tagged frames with VLAN IDs**: accept frames tagged with the specified VLAN ID (trunk port configuration).

   If no VLAN ID is specified for the site, IP Service Activator uses the VLAN ID specified for the TLS.

Incoming frames belonging to VLANs that are not in the specified range are dropped.

Note: VLAN ID 1 is reserved for the default VLAN (that all unconfigured ports belong to by default). Any traffic tagged with VLAN 1 can be transported to another port in VLAN 1 only.

Associating a Physical Component with a Layer 2 Site

Every layer 2 site must have, at minimum, the port on the relevant PE device linked to it.

For more information, see "Planning a TLS".

To link a PE access interface to a layer 2 site:

1. Drag and drop the appropriate access interface on the PE (gateway) device on to the site.

Linking Sites to a TLS

You define the access points to the TLS by linking the appropriate customer sites to the TLS object:

- A “port-based” site may be linked to a port-based TLS.
- A “port and VLAN”-based site may be linked to a port and VLAN-based TLS.

To link a site to a TLS:

1. Drag and drop the layer 2 site object onto the TLS to create a link.

Implementing a TLS

After the site and TLS details are set up, the entire configuration can be applied by committing the transaction.

When you commit the transaction, any concrete TLSs that will be created are listed in the Concretes page of the Transaction dialog box.

Any validation errors are reported in the Transaction dialog box and the Current Faults pane.

If you wish to cancel the transaction after reviewing the concrete TLSs that will be created and the faults generated by the transaction, click **Cancel**.

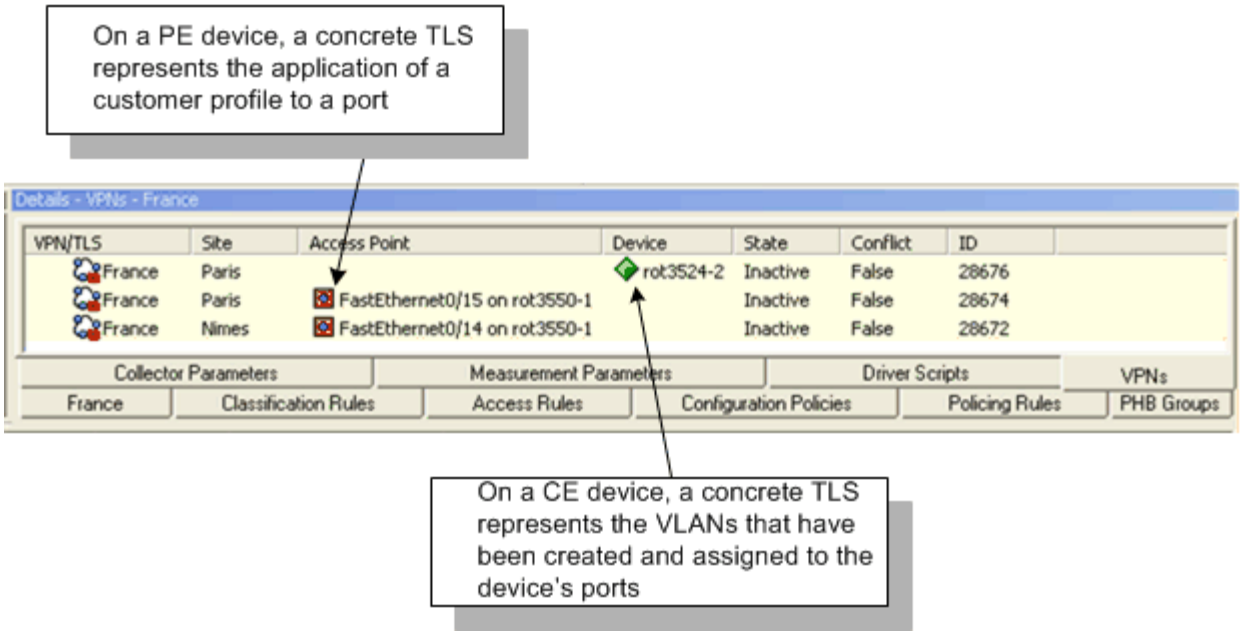
If you wish to proceed with the transaction, click **OK**. Configuration details are sent to the proxy agent/Network Processor and on to the appropriate device driver/cartridge. For more information about committing a transaction, see *IP Service Activator User’s Guide*.

Viewing Implemented TLSs

You can view a list of the TLSs that have been propagated to the network and installed on an interface.

By viewing concrete TLS details for a TLS object, you can view the points in the network at which TLS or VLAN configuration has been applied, as illustrated in Figure 6–6.

Figure 6–6 Concrete TLS Details



To view implemented TLS details:

1. Double-click on the relevant object from the hierarchy tree or the topology map:

   You can view concrete TLSs for:

   - A port on a PE device represents the application of a TLS service to a specific port
   - A TLS represents the points in the network at which TLS configuration has been applied

2. In the Details pane, select the **VPNs** tab to view details of the TLS configuration that applies to the port on PE devices.

7

Configuring IPsec

This chapter explains how to configure IPsec using Oracle Communications IP Service Activator.

About VRF-Aware IPsec

IP Service Activator allows you to configure VRF-Aware IPsec tunnels using the following configuration policies:

- Customer IPsec Access
- Public IPsec

The VRF-Aware IPsec feature allows you to map IPsec tunnels that terminate on a shared public interface to specific Virtual Routing and Forwarding (VRF) instances. This allows you to map IPsec tunnels to MPLS VPNs extending customer VPN access to users that are not directly reachable via dedicated WAN links.

VRF-Aware IPsec Procedures and Configuration Policies

For details on implementing VRF-Aware IPsec using the IP Service Activator including step-by-step procedures, refer to the IP Service Activator Online Help.

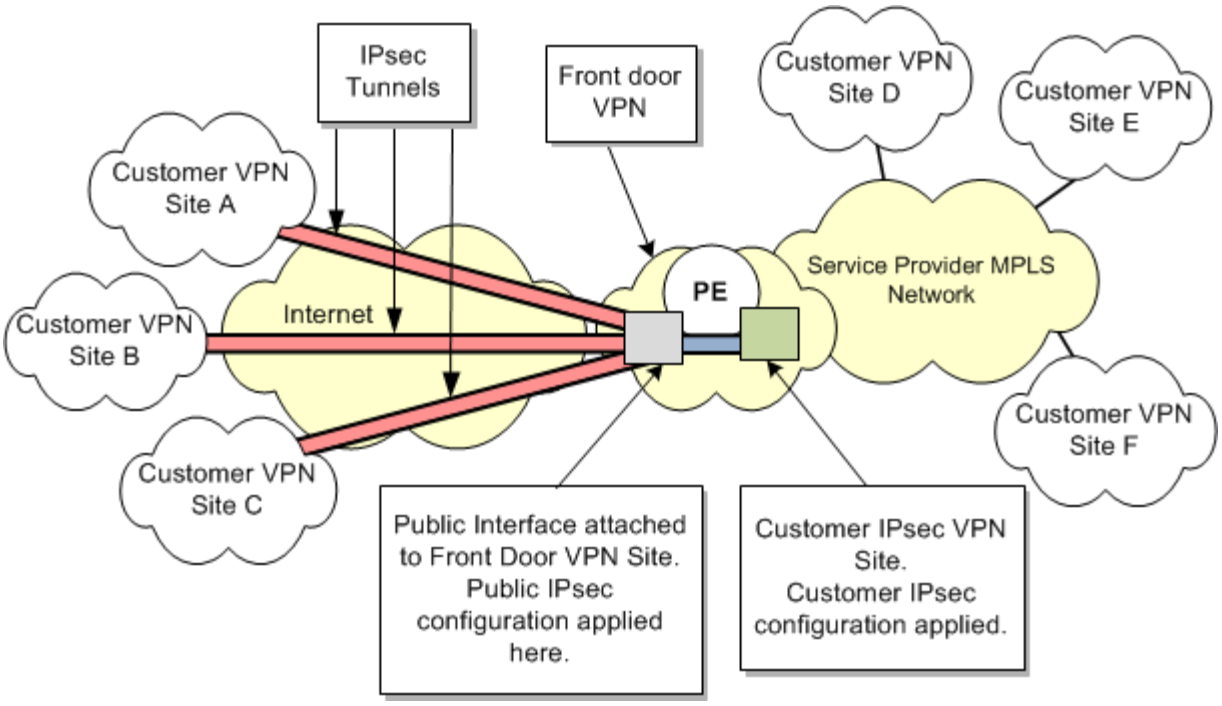
VRF-aware IPsec topics in the Online Help include:

- VRF-Aware IPsec - Concepts and Examples
- Creating a redundant Front Door VRF configuration
- Creating a Front Door VPN and Site
- Creating a Customer IPsec Site
- Configuration Policy - Customer IPsec Access
- Configuration Policy - Public IPsec

Example of VRF-Aware IPsec Implementation

Figure 7–1 illustrates an example VRF-Aware IPsec implementation.

Figure 7–1 VRF-Aware IPsec Implementation



A service provider has an MPLS-enabled core network and provides a customer with VPN access between customer sites D, E, and F.

Additional remote customer VPNs (with customer sites A, B, and C) lie outside the service provider's core network. These remote sites are not directly attached to the WAN supporting the Customer MPLS VPN. Instead, they are connected to the service provider's MPLS network through an untrusted intermediary, such as an unsecured Internet connection.

In order to connect customer sites A, B, and C to the customer VPN provisioned in the MPLS-enabled core network, IPsec tunnels are provisioned across the untrusted intermediary connection.

These tunnels deliver encrypted data to a PE router (PE1). Incoming packets are decrypted and passed on through the Customer VPN on the service provider's MPLS network. Similarly, packets arriving at PE1 from the customer VPN which are destined for sites A, B or C, are encrypted at PE1 and sent over the IPsec tunnels, to be decrypted at the target site.

VRF-Aware IPsec Details

Traffic moving from Customer Sites A, B and C to Customer VPN Sites D, E, and F, is encrypted at the start of the IPsec tunnels. Packets travel from these IPsec sites over a publicly accessible network such as the Internet, through the IPsec tunnels to the public interface (2) on PE1.

The public interface is included in the Front Door VPN Site and this is where the packets are decrypted.

At the Customer IPsec site, which is a member of both the Front Door VPN, and the Customer VPN on the service provider's MPLS network, the appropriate MPLS labelling is applied for the packets to be transported over the Customer MPLS VPN.

Going in the other direction, MPLS-labelled packets arrive at the Customer IPsec site. At the Customer IPsec site, the MPLS labels are stripped and the packets are passed to the Front Door site. At the Front Door site (which includes the public interface), the packets are encrypted for transport over the IPsec tunnels. At the target Customer Sites, at the ends of the IPsec tunnels, the packets are decrypted.

The IPsec tunnels configured between the Remote Sites and the PE device connect to the PE through the same public interface (labelled 2 on the diagram) at the Front Door Site in the Front Door VPN.

Configuration of the Front Door Site is performed using the Public IPsec configuration policy.

The Customer IPsec Site (labelled 3) is a member of both the Front Door VPN and the Customer MPLS VPN. The PE device containing the public interface is associated with Customer IPsec Site.

Configuration of the Customer Site is performed using the Customer IPsec configuration policy.

To support the connection between the end of an IPsec tunnel and the customer VPN in the service provider MPLS network, a small VPN, known as the Front Door VPN, is used. There are two VRF instances inside this VPN:

- A Front Door VRF (F-VRF) at the Front Door site
- A Customer VRF (C-VRF) at the Customer IPsec site

The Front Door VRF is used to isolate the public interface from the global routing tables on the PE. The Customer VRF provides connectivity to the Customer MPLS VPNs.

One or more IPsec tunnels can be attached to the PE using a single public interface. The tunnels then terminate at the appropriate C-VRF. The C-VRF for each of the IPsec tunnels may be different depending on the VRF referenced from the customer specific IPsec configuration.

IP Service Activator's VRF-Aware IPsec provisioning support includes:

- For the MPLS VPN portion, provisioning and activation of Customer VPN Sites and VPNs.
- For the IPsec portion, provisioning and activation of IPsec configuration policies and their association to the Front Door Site and specific Customer MPLS VPN sites.

For step-by-step procedures on how to provision VRF-aware IPsec, refer to the Online Help. See "VRF-Aware IPsec Procedures and Configuration Policies" for the list of available topics.

Using Configuration Policies for IPsec Provisioning

In order to use the Public IPsec and Customer IPsec configuration policies, the .policy file containing these policies must be loaded into IP Service Activator.

To load the IPsec configuration policy files:

1. Right-click on your Domain and select **Properties**.
2. On the Domain dialog box, select the **Setup** property page.
3. Browse to the **IPSecPolicyTypes.policy** file. Click **Load**.
4. Click **OK** and commit the transaction.

For step-by-step procedures on how to provision VRF-aware IPsec, refer to the Online Help. See "VRF-Aware IPsec Procedures and Configuration Policies" for the list of available topics.

8

Registering Interface Policies and Creating Interfaces

This chapter provides some practical examples of how to register and use the interface management configuration policies to create interfaces in Oracle Communications IP Service Activator.

> **Note:** Before creating any Interface Policy Registration, you must load the I**nterfaceManagementPolicyTypes.policy** file on the Domain dialog box.
>
> For information about configuration policies, see *IP Service Activator QoS User's Guide*.

About Interface Creation and Decoration

An Interface Decoration Policy allows you to configure an existing interface or sub-interface. The Decoration Policy cannot be applied to an interface that has been created by a Creation Policy. You cannot directly use the interface management configuration policies to take over management and ownership of an existing interface that has been decorated but not created using the interface management configuration policies. In this case, you must delete the sub-interface in the object model and re-create it using the interface management configuration policies.

> **Note:** As this deletes and recreates the interface object in the object model, all service associations with the interface are lost. These associations must be recreated.

For more information on creating and decorating interfaces or sub-interfaces, see the IP Service Activator online Help.

Example of Creating and Removing a Cisco Serial Sub-interface

This example illustrates the following:

- Registering Interface Creation Configuration Policies
- Creating a Sub-interface
- Removing a Sub-interface

Registering Interface Creation Configuration Policies

To register an interface creation configuration policy:

1. On the Policy tab, right-click the **Interface Policy Registrations** folder and select **Add Interface Policy Registration**.
2. On the Interface Policy Registration dialog box, specify the following attributes with their corresponding values:
   - **Name**: frSubInterfaceDataCreate
   - **Action**: Create
   - **Menu Text**: Serial Subinterface
   - **Policy Type**: Frame Relay Interface
   - **Applied Context**: Interface
   - **Vendor Name**: Cisco (9)
   - **SNMP ifType**: 32 (frameRelay)
   - **Interface Pattern**: Serial
3. Display the Creation Template property page by selecting **Creation Template**. Specify the additional attributes:
   - **SNMP ifType**: 32 (frameRelay)
   - **Speed**: 0

     The Speed attribute is used to set the initial interface speed value in the Object Model, but is not used for configuration of the device or interface. The object model value is automatically updated when the interface is discovered.
   - **Interface Name Prefix**: Select **Get prefix from parent**
4. Click **OK**.
5. Commit the transaction.

Creating a Sub-interface

Before creating a sub-interface, create a parent interface by doing one of the following:

- Discover the parent interface from the network
- Create an interface using a registered interface configuration policy

To create a sub-interface:

1. For a managed device, select the appropriate device and interface roles.
2. Right-click a serial interface and select **Add Sub-Interface** from the context menu.
3. Select the **Serial Subinterface** option created by the newly registered Interface Policy Registration.

   The New Sub-interface dialog box appears with the contents of the frSubinterfaceData configuration policy.

> **Note:** The encapsulation of the parent interface must be set to Frame Relay (**ifType frameRelay(32)**). The Add Sub-Interface menu does not appear if the Serial interface type is **prepPointToPointSerial(22)** or **ppp(23)**. To change the interface encapsulation, configure the parent interface with encapsulation frame relay and rediscover the device.

4. On the New Sub-interface dialog box, specify the sub-interface data as required.
   - **Name**: *Serial0/1/3.2* (mandatory field)
   - **Data Link Connection Identifier (dlci)**: *16* (mandatory field)
5. Select **Role**.

   The Role property page appears.
6. Select the interface role as required. If the role is not set, the interface will not be created.
7. Click **OK**.
8. Commit the transaction.

   The following Serial sub-interface is created on the device:

```
2007-09-06 20:02:14|10.156.68.126|interface Serial0/1/3.2 point-to-point
2007-09-06 20:02:14|10.156.68.126|frame-relay interface-dlci 16
2007-09-06 20:02:14|10.156.68.126|interface Serial0/1/3.2 point-to-point
2007-09-06 20:02:14|10.156.68.126|exit
```

Removing a Sub-interface

To remove a sub-interface:

1. Select the sub-interface.
2. Right-click the sub-interface and select **Delete** from the context menu.
3. Commit the transaction.

If the sub-interface object is deleted from the IP Service Activator object model, the sub-interface on the device is also removed.

Example of Decorating and Removing a Cisco Serial Sub-interface

This example illustrates the following:

- Creating an Interface Policy Registration
- Decorating an Existing Sub-interface
- Removing a Sub-interface Decoration

Creating an Interface Policy Registration

To create an Interface Policy Registration:

1. On the Policy tab, right-click the I**nterface Policy Registrations** folder and select **Add Interface Policy Registration** from the context menu.

   The Interface Policy Registration dialog box is displayed.
2. Specify the following attributes with the corresponding values:

- **Name**: ciscoUniversalInterfaceDecorateFrameRelay
- **Action**: Decorate
- **Menu Text**: Interface Settings
- **Policy Type**: Cisco Universal Interface
- **Applied Context**: Sub-Interface
- **Vendor Name**: Cisco (9)
- **SNMP ifType**: 32 (frameRelay)

3. Click **OK**.
4. Commit the transaction.

Decorating an Existing Sub-interface

To decorate a sub-interface:

1. For a managed device, specify the appropriate device and interface roles.
2. Right-click a Serial sub-interface and select **Configure Sub-interface** from the context menu.
3. Select the **Interface Settings** option created by the newly registered Interface Policy Registration.

   The Sub-interface dialog box appears with the contents of the Cisco Universal Interface configuration policy.
4. Specify the sub-interface data as required.
5. Click **OK**.
6. Commit the transaction.

Removing a Sub-interface Decoration

To remove a sub-interface decoration:

1. Right-click a decorated Serial sub-interface and select **Configure Sub-interface** from the context menu.
2. Deselect the **Interface Settings** option.
3. Commit the transaction.

   The decorated settings will be removed from the interface.

> **Note:** Deleting a decorated interface from the IP Service Activator object model will remove the decorated configuration from the device, but will not remove the interface. The interface will be recreated in the object model the next time the device is re-discovered.

Example of a Cisco Channelized Serial Interface

This example illustrates the following:

- Creating an Interface Policy Registration
- Configuring the E3 controller

- Creating a channellized Serial interface
- Removing a channellized Serial interface

Before creating a channelized serial interface, perform the following preconfiguration tasks:

1. Modify the **Config/AutoDiscovery.cfg** file to enable controller discovery.
2. Follow the Controller Discovery comments in the **AutoDiscovery.cfg** file to comment and uncomment the appropriate lines.
3. Restart the Policy Server.
4. Discover the device.

The controllers are discovered on the device as a special interface type with a different icon.

For more information about customizing discovery using **AutoDiscovery.cfg**, see *IP Service Activator User's Guide*.

Creating an Interface Policy Registration

To create an Interface Policy Registration:

1. On the Policy tab, right-click the **Interface Policy Registrations** folder and select **Add Interface Policy Registration** from the context menu.

   The Interface Policy Registration dialog box appears.
2. Specify the following attributes with the corresponding values:
   - **Name**: e3ChannellizedSerialInterfaceCreateFrameRelay
   - **Action**: Create
   - **Menu Text**: E3 Channellized Serial Interface Frame Relay
   - **Policy Type**: E3 Channelized Interface
   - **Applied Context**: Device
   - **Vendor Name**: Cisco (9)
3. Select **Creation Template**.

   The Creation Template property page is displayed.
4. Specify the additional attributes:
   - **SNMP ifType**: 32 (frameRelay)
   - **Speed**: 0
   - **Interface Name Prefix**: Serial
5. Define the Interface, Sub-Interface and VC Capabilities by doing one of the following:
   - Manually selecting on the **Interface Capabilities**, **Sub-Interface Capabilities** and **VC Capabilities** tabs
   - Using the capabilities of an existing interface by dragging an existing interface object onto the Interface Policy Registration Object.

   These are the capabilities that get assigned in the object model when the device level interface is created.

6. Click **OK**.
7. Commit the transaction.

Configuring the E3 Controller

Before configuring the E3 Controller, perform the following preconfiguration tasks:

1. On the Policy tab, expand the **Policy Types folder**, expand **Service**, then select **General**.
2. Right-click the **General** folder and select **Add Policy Type**.

   The General\- Policy Type dialog box is displayed.
3. Click **Import HTML**, and under the **SamplePolicy** folder, select **e3Controller.html**.
4. In the Name field, specify the name of the policy type.
5. Click **OK**.
6. Commit the transaction.

To configure the E3 Controller:

1. Right-click the E3 Controller and select **Add Configuration Policy** from the context menu.
2. Select **General**, then select **e3Controller**.
3. On the Configuration Policy dialog box, provide a suitable descriptive name for the configuration policy.
4. Specify the policy attributes to configure the E1 line.
5. Add a new configuration policy for each E1 line as follows:
   - **Name**: E3 0/1/0.1
   - **E1 Number**: 1
   - **Clock Source**: internal
6. Select Role.

   The Role property page is displayed.
7. Select the configuration policy role.
8. Click **OK**.
9. Repeat steps 1–8 for each E1 Line to be configured.
10. Commit the transaction.

The following figure illustrates the configuration policies for the controller E3 0/1/0:

- e1 1 clock source internal
- e1 3 clock source internal
- e1 6 clock source internal

Creating a Channelized Serial Interface

The e3ChannellizedSerialInterface interface creation policy is used to create a new Serial interface on a device, based on the Interface Registration Policy defined in "Creating an Interface Policy Registration".

To create a channellized Serial interface:

1. Right-click the device and select **Add Interface** from the context menu.
2. Select **E3 Channellized Serial Interface Frame Relay**.

   The New Interface dialog box appears with the contents of the e3ChannellizedSerialInterface configuration policy.
3. Set the interface data as required.

   The encapsulation field should be set to match the encapsulation applicable to the ifType defined in the interface policy registration to ensure the created interface capabilities are aligned.

   - propPointToPointSerial(22): HDLC
   - ppp(23): ppp
   - frameRelay(32): Frame Relay, Frame Relay IETF
4. For the e3ChallenlizedSerialInterface interface creation, the time slots filed must be configured as follows:

   - Name: Serial0/1/0/1.1
   - Encapsulation: Frame Relay
   - Time Slots: 1-5
5. Select the interface role.
6. Click **OK**.
7. Commit the transaction.

IP Service Activator creates the new interface on the device and configures allocated time slots in the E3 controller, as shown below:

```
2007-09-11 22:04:24|10.156.68.204|controller E3 0/1/0
2007-09-11 22:04:25|10.156.68.204|e1 1 channel-group 1 timeslots 1-5
2007-09-11 22:04:25|10.156.68.204|exit
2007-09-11 22:04:25|10.156.68.204|interface Serial0/1/0/1:1
2007-09-11 22:04:25|10.156.68.204|encapsulation frame-relay
2007-09-11 22:04:26|10.156.68.204|exit
```

Removing a Channelized Interface

To remove the channelized interface:

1. Select the channelized interface.
2. Right-click the channelized interface and select **Delete** from the context menu.

Deleting the interface from the IP Service Activator object model will remove the Channelized interface from the device, as shown below:

```
2007-09-11 22:07:43|10.156.68.204|no interface Serial0/1/0/1:1.1
2007-09-11 22:07:43|10.156.68.204|interface Serial0/1/0/1:1
2007-09-11 22:07:43|10.156.68.204|no encapsulation
2007-09-11 22:07:43|10.156.68.204|exit
2007-09-11 22:07:43|10.156.68.204|controller E3 0/1/0
2007-09-11 22:07:44|10.156.68.204|no e1 1 channel-group 1
2007-09-11 22:07:44|10.156.68.204|exit
```

Note: Any child sub-interface of the channelized interface is also automatically removed, both from the object model and the device.

A

Setting Up Management and Customer VPNs

This appendix outlines the high-level steps you need to follow in order to set up management and customer VPNs on Oracle Communications IP Service Activator.

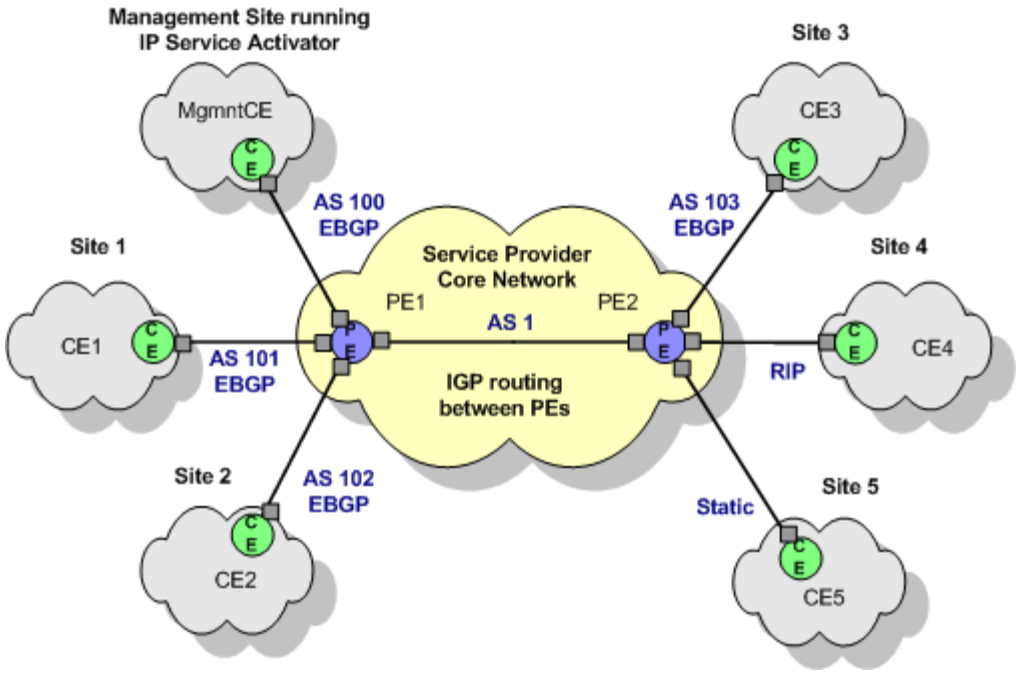
Introduction

In the following example, three VPNs are created:

- A management VPN is set up comprising the Management site and all other sites in all VPNs managed by IP Service Activator. With IP Service Activator running at the management site, all CE routers can be managed. The management site is a hub site; all other sites are spoke sites.
- Customer VPN 1 comprises sites 1, 2 and 4.
- Customer VPN 2 comprises sites 1, 3 and 5.

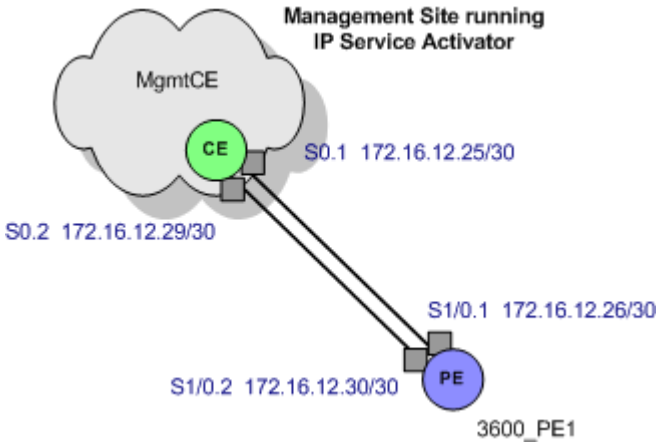
VPN 1 and 2 are both fully-meshed. The network layout and routing protocols are shown in Figure A–1.

Figure A–1 Network and Routing Protocols for Management and Customer VPNs



Between the management site and the core network, two links are required, one to provide VPN connectivity and one to provide routes to the Service Provider backbone IGP. These links are illustrated in Figure A–2.

Figure A–2 Links Between Management Site and Core Network



Configuring the VPNs

The following steps explain the sequence of operations required to set up a management VPN, enabling access to the CE routers, followed by customer VPNs. For full details, see the detailed explanation in "Setting Up MPLS VPNs".

Configuring VPNs involves:

1. Setting Up the Domain
2. Setting Up the Core Network ASN
3. Discovering the Network and Assigning Roles
4. Disabling Interfaces on CE-PE Link
5. Setting Devices to Managed
6. Setting Up Customers and Sites
7. Linking Physical Network Components with Sites
8. Setting the VPN Routing Parameters
9. Creating the Management VPN
10. Implementing the Management VPN
11. Setting Up the CE Devices
12. Setting Up the Customer VPNs
13. Implementing the Customer VPNs

Setting Up the Domain

To set up the domain:

1. On the Domain page of the Domain dialog box:
   - Set the Type to **MPLS VPN**.

- Select the **PE to CE Addresses** option.

2. Set the required parameters on the VPN BGP page and the VPN MPLS page.

   See "Setting Up Domain Parameters" for more details.

Setting Up the Core Network ASN

To set up the core network ASN:

1. On the ASN page of the Domain dialog box, set the internal BGP ASN to **1**.

   See "Setting Up the Provider Core ASN for the Domain" for more details.

Discovering the Network and Assigning Roles

To discover the network and assign roles to devices and interfaces:

1. Run a device discovery to discover the PE devices (PE1 and PE2) and the CE device at the management site (MgmtCE).

   Devices can be discovered using their IP addresses or DNS names.

2. Assign the correct system-defined roles to devices. Routers must be assigned the **Gateway** role and the CE router must be assigned the **Access** role.

   Appropriate interfaces on the devices also need to be assigned **Local** or **Access** roles.

3. Assign roles manually for each device.

   For more information, see *IP Service Activator User's Guide*.

Disabling Interfaces on CE-PE Link

To prevent interfaces on a CE-PE link from being configured into a VPN, disable them.

To disable interfaces:

1. Assign the role of **Disabled** to the interfaces at both ends of the Serial 0.1 link between PE1 and MgmtCE (the link that is not to be used for the VPN connection).

> **Note:** The Access Point (interface or sub-interface) that is in the Management VPN and thus provides routes to the CE must be passive. This is so that routes from the customer networks are not leaked into the Service Provider backbone, and vice versa

Setting Devices to Managed

Set all discovered devices to **Managed** so that IP Service Activator can configure them.

Setting Up Customers and Sites

To set up customers and sites:

1. On the Service tab, set up the appropriate customers:

   - Create a dummy customer, such as **Management** for the management VPN
   - Create dummy customers, **Customer 1** and **Customer 2**, for the customer VPNs

2. Create site objects for the management site and each of the customers sites and give them identifying names.

Linking Physical Network Components with Sites

For each site, link the appropriate access interface on the PE router to the site by dragging and dropping.

Setting the VPN Routing Parameters

To set up VPN routing parameters for each site:

1. On the Site property page, set the appropriate routing type and relevant parameters (EBGP, RIP, OSPF, EIGRP, EBGP & OSPF, EBGP & RIP, EBGP & EIGRP and/or static routing).
2. On the Addressing page of the Site dialog box, set up private addresses (used with the VPN) and public addresses (used outside the VPN).

Note: In this example, it is assumed that the settings on the Advanced VPN page are left as defaults.

Creating the Management VPN

To create the management VPN:

1. Under the Management customer object, create a VPN object to represent the management VPN.
2. Link all the sites (Management site, Site 1, Site 2, Site 3, Site 4, and Site 5) to the VPN by dragging and dropping.
3. On the Connectivity page of the VPN properties, set the Connectivity to **Management**.
4. Ensure that the management site is selected as the hub site.

Implementing the Management VPN

To implement the management VPN:

1. Save the changes to the database.
2. Commit the transaction.

Setting Up the CE Devices

To set up the CE devices:

1. Discover the CE devices using their defined loopback addresses.
2. Link the CE devices to the appropriate sites by dragging and dropping.

   An error is flagged if the devices are not linked.

Setting Up the Customer VPNs

To set up the customer VPNs:

1. On the Service tab, create to VPN objects to represent the two customer VPNs.

2. Link the customer sites to the appropriate VPN objects by dragging and dropping:
   - Link Customer VPN 1 to Site 1, Site 2, and Site 4.
   - Link Customer VPN 2 to Site 1, Site 3, and Site 5.

Implementing the Customer VPNs

To implement the customer VPNs:

1. Save the changes to the database.
2. Commit the transaction.

> **Note:** For example VPN configurations, see the Device Driver guide appropriate for your installation.