



CHAPTER 2

Setting Up the ISC Services

This chapter contains the basic steps to set up the Cisco IP Solution Center (ISC) services to support MPLS VPN service policies and service requests. It contains the following sections:

- [Overview, page 2-1](#)
- [Creating Devices, page 2-2](#)
- [Creating Customers, Sites, and CPEs, page 2-7](#)
- [Creating Providers, Regions, and PEs, page 2-9](#)
- [Creating Access Domains, page 2-12](#)
- [Creating Resource Pools, page 2-15](#)
- [Defining VPNs, page 2-22](#)
- [Creating CE Routing Communities, page 2-32](#)



Note

This chapter presents high-level information on ISC services that are relevant to MPLS VPN. For more detailed information on setting up these and other basic ISC services, see the [Cisco IP Solution Center Infrastructure Reference, 5.1](#). How to create the associated elements in ISC is explained in the chapter, Service Inventory—Inventory and Connection Manager, and how to discover devices is explained in the chapter, Service Inventory—Discovery, in the [Cisco IP Solution Center Infrastructure Reference, 5.1](#).

Overview

To create an MPLS VPN service request, you must create the following infrastructure data:

- **Devices**

A Device in ISC is a logical representation of a physical device in the network. You can import devices (configurations) into ISC by using Inventory Manager or the ISC GUI. You can also use the Auto Discovery feature of Inventory Manager to import devices into the Repository.
- **Customers**

A customer is typically an enterprise or large corporation that receives network services from a service provider. A Customer is also a key logical component of ISC.

 - **Sites**

A Site is a logical component of ISC that connects a Customer with a CE. It can also represent a physical customer site.

- CPE/CE Devices

A CPE is “customer premises equipment,” typically a customer edge router (CE). It is also a logical component of ISC. You can create CPE in ISC by associating a device with a Customer Site.
- Providers

A provider is typically a “service provider” or large corporation that provides network services to a customer. A Provider is also a key logical component of ISC.

 - Regions

A Region is a logical component of ISC that connects a Provider with a PE. It can also represent a physical provider region.
 - PE Devices

A PE is a provider edge router or switch. It is also a logical component of ISC. You can create PE in ISC by associating a Device with a Provider Region. In ISC, a PE can be a “point of presence” router (POP) or a Layer 2 switch (CLE).
- Access Domains (for Layer 2 Access)

The Layer 2 Ethernet switching domain that connects a PE to a CE is called an Access Domain. All the switches attached to the PE-POP belong to this Access Domain. These switches belong to the Provider and are defined in ISC as PE-CLE.
- Resource Pools
 - IP Addresses
 - Multicast
 - Route Distinguisher
 - Route Target
 - VLANs (for Layer 2 Access)
- VPN

Before creating a Service Policy, a VPN name must be defined within ISC.
- CE Routing Communities (CERC is optional)

Creating Devices

This section describes how to create a Device with the ISC GUI, connect to a Cisco IOS router in the network, collect the live configuration, and populate the Repository. This section covers the following topics:

- [Creating Logical Devices, page 2-3](#)
- [Collecting Configurations, page 2-4](#)
- [Monitoring Task Logs, page 2-5](#)
- [Setting Up Devices for IOS XR Support, page 2-6](#)

Creating Logical Devices

To create a logical device, perform the following steps.

Step 1 Choose **Service Inventory > Inventory and Connection Manager > Devices**.

The Devices window appears.

Step 2 Click **Create**.

Step 3 From the drop-down list, choose **Cisco Device**.

The Create Cisco Device window appears, as shown in [Figure 2-1](#).

Figure 2-1 New Device Information

Create Cisco Device

General

Device Host Name* :

Device Domain Name:

Description:

Collection Zone:

Management IP Address:

Interfaces:

Associated Groups

Login and Password Information

Login User:

Login Password:

Verify Login Password:

Enable User:

Enable Password:

Verify Enable Password:

Device and Configuration Access Information

Terminal Session Protocol:

Config Access Protocol:

OS:

SNMP Version:

SNMP v1/v2c

Community String RO:

Community String RW:

Additional Properties:

Note: * - Required Field

149136

- Step 4** Enter all required information for this new device.
- Step 5** For Additional Properties, click **Show**.
- Step 6** To save this new device, click **Save**.
- You have saved a Device in the Repository.

Collecting Configurations

This section describes how to connect to the physical device in the network, collect the device information from the router, and populate the Repository. To do this, perform the following steps.

- Step 1** Choose **Monitoring > Task Manager**.
- The Tasks window appears.
- Step 2** Click **Create**.
- Step 3** Choose **Collect Config**.
- The Create Task window appears, as shown in [Figure 2-2](#).



Tip You might want to change the default **Name** and **Description** for this task, so you can more easily identify it in the task log.

Figure 2-2 Create Task

Create Task	
Name *	Collect Config 2004-01-14 (mlce3DeviceCreation)
Type:	Collect Config
Description:	Created on 2004-01-14 mlce3DeviceCreation
Task Configuration Method:	<input checked="" type="radio"/> Simplified <input type="radio"/> Advanced (via wizard)
Note: * - Required Field	

- Step 4** Click **Next**.
- The Collect Config Task window appears, as shown in [Figure 2-3](#).

Figure 2-3 Collect Config Task

Collect Config Task

Collect Config Task: Collect Config 2004-01-14 (mlce3DeviceCreation)

Devices:

Groups:

Options:

- Retrieve device attributes
- Retrieve Interfaces

Schedule:

- Now
- Later
- None

Task Owner:

- Customer
- Provider
- None

Note: * - Required Field

111576

- Step 5** To choose devices associated to the task, in the Devices panel, click **Select/De Select**.
The Select Device window appears.
- Step 6** Check to choose the desired device(s), then click **Select**.
The Collect Config Task window reappears.
- Step 7** To choose device groups associated to the task, in the Groups panel, click **Select/De Select**.
A list of available device groups appears.
- Step 8** Check to choose the desired device group(s), then click **Select**.
The Collect Config Task window reappears.
- Step 9** Set schedule and task owner, if applicable.
- Step 10** Click **Submit**.
The Tasks window appears.
- Step 11** Choose your task in the Task Name column, then click **Details** to view more information.

Monitoring Task Logs

To monitor task logs, perform the following steps.

- Step 1** Choose **Monitoring > Task Manager**.
The Tasks window appears.

- Step 2** In the Selection pane, click **Logs**.
The Task Runtime Actions window appears.



Note The **Status** field shows the task has completed successfully.

- Step 3** Choose your task and then click **Instances** to view more information.

Creating Device Groups

To create device groups, perform the following steps.

- Step 1** Choose **Service Inventory > Inventory and Connection Manager > Device Groups**.
The Device Groups window appears.
- Step 2** Click **Create**.
The Create Device Group window appears.
- Step 3** In the Name field, enter the Device Group Name.
- Step 4** Click **Save**.

Setting Up Devices for IOS XR Support

ISC supports provisioning of basic MPLS VPNs on devices running Cisco's IOS XR software. IOS XR, a new member of the Cisco IOS family, is a unique self-healing and self-defending operating system designed for always-on operation while scaling system capacity up to 92Tbps.



Note For information about specific platforms and features supported for IOS XR devices for MPLS VPN, as well as IOS XR versions supported, see the [Release Notes for Cisco IP Solution Center, 5.1](#).

To enable IOS XR support in MPLS VPN, perform the following steps.

- Step 1** Set the DCPL property **Provisioning/Service/mpls/platform/CISCO_ROUTER/IosXRConfigType** to XML.
Possible values are **CLI**, **CLI_XML**, and **XML** (the default).
- Step 2** Set the DCPL property **DCS/getCommitCLIConfigAfterDownload** to true (the default).
This allows ISC to retrieve the committed CLI configuration after an XML configuration has been downloaded. See [Viewing Configlets on IOS XR Devices, page 6-32](#) for more information.
- Step 3** Create the device in ISC as an IOS XR device, as follows:
- a. Create the Cisco device by choosing **Service Inventory > Inventory and Connection Manager > Devices > Create**.
The Create Cisco Device window appears.

- b. Set the OS attribute, located under Device and Configuration Access Information, to IOS_XR.

**Note**

For additional information on setting DCPL properties and creating Cisco devices, see the [Cisco IP Solution Center Infrastructure Reference, 5.1](#).

- Step 4** Create and deploy MPLS VPN service requests, following the procedures in this guide.

Sample configlets for IOS XR devices are provided in [Appendix A, “Sample Configlets”](#).

Creating Customers, Sites, and CPEs

In ISC, a customer is defined by the following three logical components:

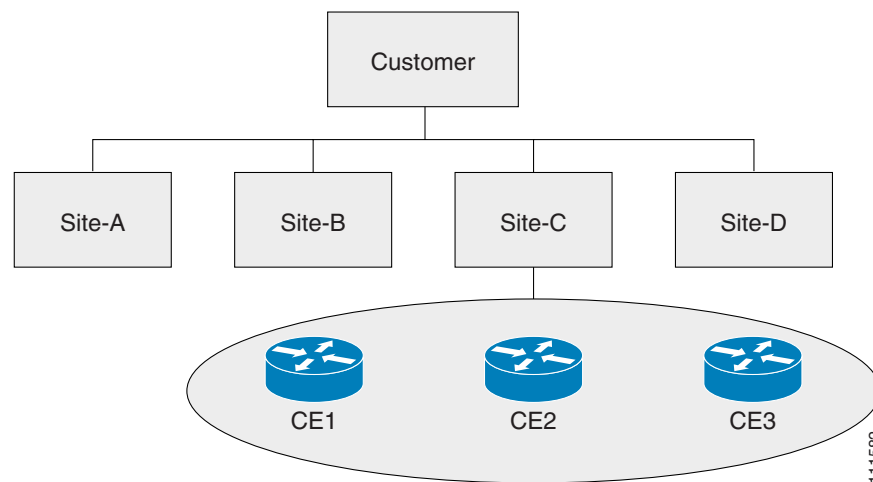
- Customer Name
- Customer Site
- Customer Device (CPE)

In ISC, a Customer is a logical container for Sites and CEs.

Within a Customer, there can be one or more Sites. Sites are logical entities that can be defined in any way that makes sense to a service provider.

[Figure 2-4](#) shows an overview of an ISC Customer.

Figure 2-4 Overview of an ISC Customer



This section describes how to create a Customer with the ISC GUI, create a Site for the Customer, and associate a Device with the Site. This section covers the following topics:

- [Creating Customers, page 2-8](#)
- [Creating Sites, page 2-8](#)
- [Creating CPEs, page 2-8](#)

Creating Customers

To create a customer, perform the following steps.

-
- Step 1** Choose **Service Inventory > Inventory and Connection Manager > Customers**.
The Customers window appears.
 - Step 2** Click **Create**.
The Create Customer window appears.
 - Step 3** Enter a Customer Name and then click **Save**.
The Customers window appears.
-

Creating Sites

To create a site, perform the following steps.

-
- Step 1** Choose **Service Inventory > Inventory and Connection Manager**.
 - Step 2** In the Selection pane, click **Customer Sites**.
The Customer Site window appears.
 - Step 3** Click **Create**.
The Create Customer Site window appears.
 - Step 4** Enter a site name in the Name field.
 - Step 5** To associate a customer to this site, in the Customer field, click **Select**.
A list of available customer names appears.
 - Step 6** Check to choose the desired customer, then click **Select**.
The Create Customer Site window reappears.
 - Step 7** Click **Save**.
-

Creating CPEs

To create a CPE device, perform the following steps.

-
- Step 1** Choose **Service Inventory > Inventory and Connection Manager**.
 - Step 2** In the Selection pane, click **CPE Devices**.
The CPE Devices window appears.
 - Step 3** Click **Create**.
The Create CPE Device window appears.

- Step 4** In the Device Name field, click **Select**.
The Select Device window appears.
- Step 5** Check to choose a device, then click **Select**.
The Create CPE Device window reappears, as shown in [Figure 2-5](#).

Figure 2-5 Create CPE Device

Create CPE Device	
Device Name *	pe1 <input type="button" value="Select"/>
Site Name *	<input type="button" value="Select"/>
Management Type:	Unmanaged Multi-VRF
Pre-shared Keys:	<input type="button" value="Edit"/>
IPsec Public IP Address:	<input type="text"/>
IP Address Ranges:	<input type="button" value="Edit"/>

- Step 6** From the drop-down list, choose a Management Type (**Unmanaged Multi-VRF**).
- Step 7** Click **Save**.
The Create CPE Device window appears showing the Unmanaged Multi-VRF CPE Device you have created.

Creating Providers, Regions, and PEs

In ISC, a Provider is defined by the following three logical components:

- Provider name and BGP Autonomous System (AS) number
- Provider region
- Provider edge device (PE)

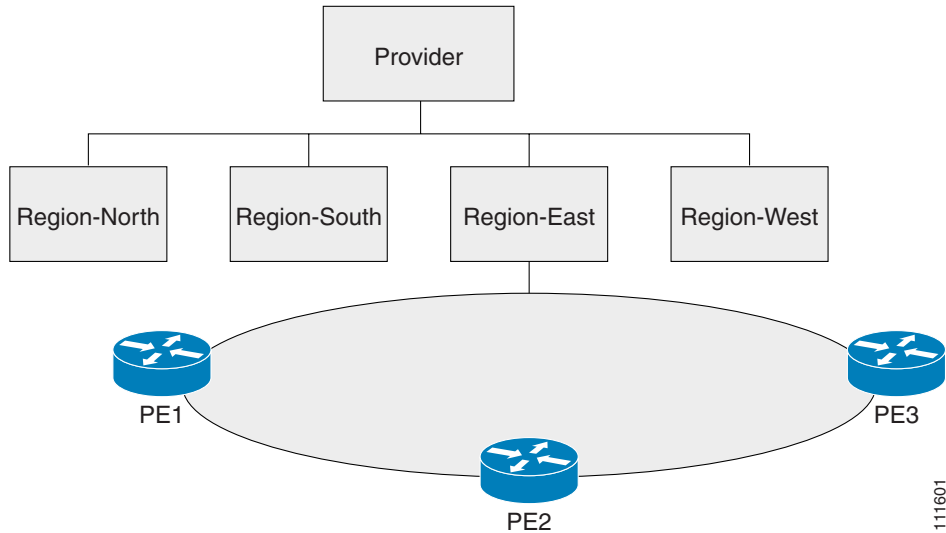
In ISC, a provider administrative domain (PAD) is a single AS. It is not a specific service provider, rather it is a logical container for Regions and PEs.

Within a single PAD, there must be one or more Regions. Regions are logical entities that can be defined in any way that makes sense to a service provider.

Within a Region, a Provider can contain one or more PEs. The PEs can be a PE-POP (“router”) or a PE-CLE (“switch”).

[Figure 2-6](#) shows an overview of an ISC Provider.

Figure 2-6 Overview of an ISC Provider



This section covers the following topics:

- [Creating a Provider, page 2-10](#)
- [Creating a Region for PE, page 2-11](#)
- [Creating PEs, page 2-11](#)
- [Editing PEs, page 2-12](#)

Creating a Provider

To create a provider, perform the following steps.

-
- Step 1** Choose **Service Inventory > Inventory and Connection Manager > Providers**.
The Providers window appears.
- Step 2** Click **Create**.
The Create Provides window appears.
- Step 3** In the Name field, enter a provider name.
- Step 4** In the BGP AS (Border Gateway Protocol Autonomous System) field, enter a a valid value (1-65535).
- Step 5** Enter contact information is applicable.
- Step 6** Click **Save**.
-

Creating a Region for PE

To create a region, perform the following steps.

-
- Step 1** In the Selection pane, click **Provider Regions**.
The Provider Regions window appears.
 - Step 2** Click **Create**.
The Create Provider Region window appears.
 - Step 3** In the Name field, enter a provider region name.
 - Step 4** In the Provider field, accept the default value, if one is shown, or to choose a provider, click **Select**.
 - Step 5** Click **Save**.
-

Creating PEs

To set up a device as a Provider Edge (PE) device, perform the following steps.

-
- Step 1** Choose **Service Inventory > Inventory and Connection Manager**.
 - Step 2** In the Selection pane, click **PE Devices**.
The PE Devices window appears.
 - Step 3** Click **Create**.
The Create PE Device window appears.
 - Step 4** In the Device Name field, click **Select**.
The Select Device window appears.
 - Step 5** Check to choose a device, then click **Select**.
The Create PE Device window reappears, as shown in [Figure 2-7](#).

Figure 2-7 Create PE Device

Create PE Device	
Device Name *	Select
PE Region Name *	Select
PE Role Type:	N-PE <input type="checkbox"/> 6VPE
Save Cancel	
Note: * - Required Field	

- Step 6** In the PE Region Name field, click **Select**.
The Select Region window appears.
- Step 7** Check to choose a region, then click **Select**.
The Create PE Device window reappears.
- Step 8** From the drop-down list, choose a PE Role Type (N-PE, U-PE, P, or PE-AGG).

**Note**

If the role type is N-PE, you can check the 6VPE check box to designate the device as a 6VPE device. See [Chapter 4, “IPv6 and 6VPE Support in MPLS VPN”](#) for more information on IPv6 and 6VPE support in ISC.

- Step 9** Click **Save**.
The PE Device window appears showing the PE device you have created.

Editing PEs

To view or edit a PE, perform the following steps.

- Step 1** Choose **Service Inventory > Inventory and Connection Manager**.
- Step 2** In the Selection pane, click **PE Devices**.
The PE Devices window appears.
- Step 3** Choose the PE Device.
- Step 4** Click **Edit**.
The Edit PE Device window appears.
- Step 5** Make required changes, then click **Save**.

Creating Access Domains

**Note**

This section is only required for Layer 2 access to MPLS VPN.

Any Transport over MPLS (AToM) is the Cisco solution for transporting Layer 2 traffic over an IP/MPLS backbone. AToM is required for supporting legacy services over MPLS infrastructures and for supporting new connectivity options, including Layer 2 VPNs and Layer 2 virtual leased lines.

AToM supports three types of Ethernet-based L2VPNs (EoMPLS):

- Point-to-Point Ethernet Wire Service (EWS)
- Point-to-Point Ethernet Relay Service (ERS)
- Multipoint TLS Service

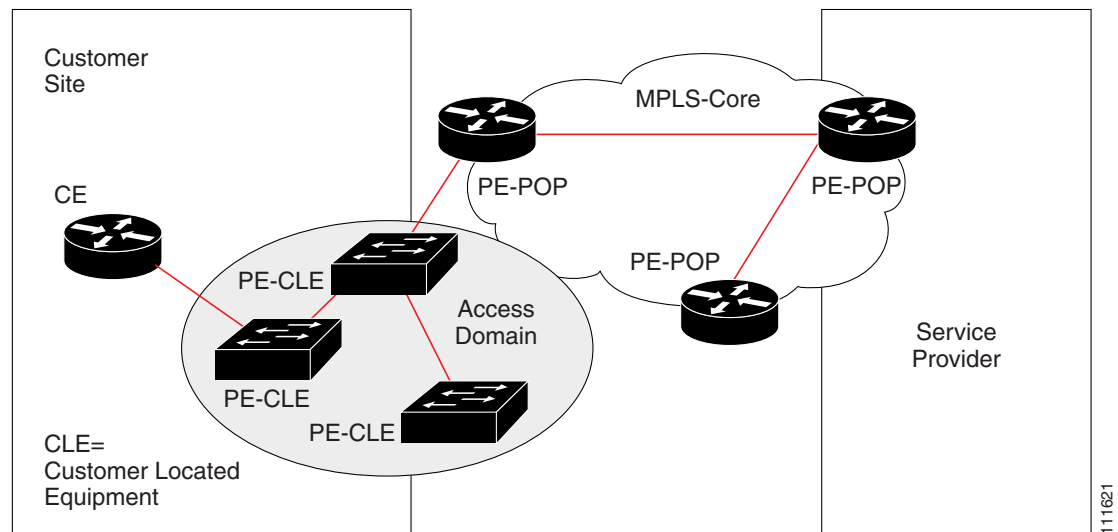
The Layer 2 Ethernet switching domain that connects a PE to a CE is called an Access Domain. All the switches attached to the PE-POP belong to this Access Domain. These switches belong to the Provider and are defined in ISC as PE-CLE.

**Note**

To have ISC automatically assign VLAN links from a VLAN pool, you must create an Access Domain.

ISC supports multiple PE-POPs per Access Domain and multiple PE-CLE devices can be included. [Figure 2-8](#) shows an overview of an ISC Access Domain.

Figure 2-8 Overview of an Access Domain



To create an Access Domain, perform the following steps.

- Step 1** Choose **Service Inventory > Inventory and Connection Manager**.
- Step 2** In the Selection pane, under **Providers**, click **Access Domains**.
The Access Domains window appears.
- Step 3** Click **Create**.
The Create Access Domain window appears, as shown in [Figure 2-9](#).

Figure 2-9 Create Access Domain

Create Access Domain

Name*:

Provider*:

PEs*:

Reserved VLANs:

#	Start	Size	Management VLAN
Showing 0 of 0 records			

Rows per page: Go to page: of 1

Note: * - Required Field

111617

Step 4 Enter an Access Domain Name.

Step 5 Choose a Provider.

Step 6 Click **Select** to show PEs.

The Show PEs window appears.

Step 7 Choose a PE.

Step 8 Click **Select**.

You are returned to the Create Access Domain window.

Step 9 For Reserved VLANs, click **Create**.

The Create Reserved VLAN window appears, as shown in [Figure 2-10](#).

Figure 2-10 Create Reserved VLAN

Starting Value*: (1 - 4094)

Size*: (1 - 4094)

Management VLAN:

Note: * - Required Field

111619

Step 10 Enter a Starting Value.

Step 11 Enter a Size.

Step 12 Check to choose **Management VLAN**.

Step 13 Click **OK**.

The Access Domains window appears showing that the Access Domain has been saved in the Repository.

Creating Resource Pools

This section describes how to create Resource Pools using the Cisco IP Solution Center (ISC) GUI. It contains the following sections:

- [Overview of Resource Pools, page 2-15](#)
- [Creating an IPv4 Address Pool, page 2-16](#)
- [Creating a Multicast Pool, page 2-16](#)
- [Creating a Route Distinguisher Pool, page 2-17](#)
- [Creating a Route Target Pool, page 2-18](#)
- [Creating a Site of Origin Pool, page 2-19](#)
- [Creating a VC ID Pool, page 2-20](#)
- [Creating a VLAN Pool, page 2-21](#)

Overview of Resource Pools

Before creating a service in ISC, you must define your Resource Pools. From these Resource Pools, ISC can automatically assign some values during the provisioning process. You can also manually assign these values during the provisioning process, but it is not recommended.

ISC allocates numbers from the following pools during the provisioning process:

- **IPv4 Address**—Connects PE and CE interfaces, when you define addresses in a service request.
- **Multicast**—Class D addresses used with multicast, when building PE to multiple CE links.
- **Route Distinguisher (RD)**—A 64-bit number composed of the Provider AS number and an index number that is prepended to a VPN route. The RD allows the route subnet to be unique across the entire provider MPLS VPN network. It is carried by MP-BGPv4 as a 96-bit VPNv4 address as part of the extended community string.
- **Route Target (RT)**—An import and export feature of a VRF, the RT allows VPN routes to be forwarded between VRFs. It is a 64-bit number, also carried as part of the MP-BGPv4 extended community string, and directly related to each VPNv4 route and its VPN-related IPv4 route.
- **Site of Origin**—Indicates the origin of a BGP update. Depending on the use of two Cisco IOS BGP commands, the Site of Origin will be used by BGP to preclude routing loops.
- **Virtual Circuit Identifier (VC ID)**—Used as a Layer 2 circuit identifier across a provider network.
- **VLAN**—Used in a Layer 2 VPN as a circuit identifier within the provider Access Domain.



Note The VLAN pool does not supply a value for a second VLAN ID, when that feature is used for Q-in-Q matching. See the section [Notes on the VLAN ID and Second VLAN ID Attributes, page 6-10](#) for additional information about second VLAN ID.

Creating an IPv4 Address Pool

To create an IPv4 address pool, perform the following steps.

Step 1 Choose **Service Inventory > Inventory and Connection Manager > Resource Pools**.

The Resource Pools window appears.

Step 2 Choose **IPv4 Address** from the Pool Type drop-down list.

Step 3 Click **Create**.

The Create IP Address Pool window appears, as shown in [Figure 2-11](#).

Figure 2-11 Create IP Address Pool

Create IP Address Pool

IP Address Pool*: 25.5.0.0/24 (IP Address/Mask)

Pool Mask (bits)*: 30 32

Pool Association*: East-X Region Select

Save Cancel

Note: * - Required Field

111641

Step 4 Enter an IP Address and Mask.

Step 5 Choose the **Pool Mask (bits)** value (**30**).



Note Use **32** for loopback addresses.

Step 6 Click **Select** to associate the pool to a Region.

The Select Region window appears.

Step 7 Choose a **Region**.

Step 8 Click **Select**.

The Create IP Address Pool window reappears.

Step 9 Click **Save**.

The Resource Pools - IP Address window appears showing that the IP Address Pool is in the Repository.

Creating a Multicast Pool

To create a multicast pool, perform the following steps.

Step 1 Choose **Service Inventory > Inventory and Connection Manager > Resource Pools**.

The Resource Pools window appears.

- Step 2** Choose **Multicast** from the Pool Type drop-down list.
The Resource Pools - Multicast window appears.
- Step 3** Click **Create**.
The Create Multicast Pool window appears, as shown in [Figure 2-12](#).

Figure 2-12 Create Multicast Pool

Create Multicast Pool

Multicast Address*: 239.0.0.0/24 (IP Address/Mask)

Use for Default MDT:

Use for Data MDT:

Save Cancel

Note: * - Required Field

111646

- Step 4** Enter an IP Address and Mask.
- Step 5** Choose the defaults (**Default MDT** and **Data MDT**).
- Step 6** Click **Save**.
The Resource Pools - Multicast window appears showing the Multicast Address Pool in the Repository.

Creating a Route Distinguisher Pool

To create a route distinguisher (RD) pool, perform the following steps.

- Step 1** Choose **Service Inventory > Inventory and Connection Manager > Resource Pools**.
The Resource Pools window appears.
- Step 2** Choose **Route Distinguisher** from the Pool Type drop-down list.
The Resource Pools - Route Distinguisher window appears.
- Step 3** Click **Create**.
The Create Route Distinguisher Pool window appears, as shown in [Figure 2-13](#).

Figure 2-13 Create Route Distinguisher Pool

Create Route Distinguisher Pool

RD Pool Start*: 0 (0 - 2147483646)

RD Pool Size*: 0 (1 - 2147483647)

Provider*: Provider-X

Note: * - Required Field

111622

Step 4 Enter an RD Pool Start value.

Step 5 Enter an RD Pool Size value.

Step 6 Click **Select**.

The Select Provider window appears.

Step 7 Choose a **Provider**.

Step 8 Click **Select**.

The Create Route Distinguisher Pool window reappears.

Step 9 Click **Save**.

The Resource Pools - Route Distinguisher window appears showing the Route Distinguisher Pool in the Repository.

Creating a Route Target Pool

To create a route target (RT) pool, perform the following steps.

Step 1 Choose **Service Inventory > Inventory and Connection Manager > Resource Pools**.

The Resource Pools window appears.

Step 2 Choose **Route Target** from the Pool Type drop-down list.

The Resource Pools - Route Target window appears.

Step 3 Click **Create**.

The Create Route Target Pool window appears, as shown in [Figure 2-14](#).

Figure 2-14 Create Route Target Pool

Create Route Target Pool

RT Pool Start*: (0 - 2147483646)

RT Pool Size*: (1 - 2147483647)

Provider*:

Note: * - Required Field

111626

- Step 4** Enter an RT Pool Start value.
- Step 5** Enter an RT Pool Size value.
- Step 6** Click **Select**.
- The Select Provider window appears.
- Step 7** Choose a **Provider**.
- Step 8** Click **Select**.
- The Create Route Target Pool window reappears.
- Step 9** Click **Save**.
- The Resource Pools - Route Target window appears showing the Route Target Pool in the Repository.

Creating a Site of Origin Pool

To create a site of origin (SOO) pool, perform the following steps.

- Step 1** Choose **Service Inventory > Inventory and Connection Manager > Resource Pools**.
- The Resource Pools window appears.
- Step 2** Choose **Site of Origin** from the Pool Type drop-down list.
- The Resource Pools - Site of Origin window appears.
- Step 3** Click **Create**.
- The Create Site of Origin Pool window appears, as shown in [Figure 2-15](#).

Figure 2-15 Create Site of Origin Pool

Create Site of Origin Pool

SOO Pool Start*	50000	(0 - 2147483646)
SOO Pool Size*	1000	(1 - 2147483647)
Provider*	Provider-X	Select

Save Cancel

Note: * - Required Field

11:16:30

Step 4 Enter an SOO Pool Start value.

Step 5 Enter an SOO Pool Size value.

Step 6 Click **Select**.

The Select Provider window appears.

Step 7 Choose a **Provider**.

Step 8 Click **Select**.

The Create Site of Origin Pool window reappears.

Step 9 Click **Save**.

The Create Route Target Pool window appears showing a Site of Origin Pool in the Repository.

Creating a VC ID Pool

To create a VC ID pool, perform the following steps.

Step 1 Choose **Service Inventory > Inventory and Connection Manager > Resource Pools**.

The Resource Pools window appears.

Step 2 Choose **VC ID** from the Pool Type drop-down list.

The Resource Pools - VC ID window appears.

Step 3 Click **Create**.

The Create VC ID Pool window appears, as shown in [Figure 2-16](#).

Figure 2-16 Create VC ID Pool

Step 4 Enter an VC Pool Start value.

Step 5 Enter an VC Pool Size value.

Step 6 Click **Save**.

The Resource Pools - VC ID window appears showing a VC ID Pool in the Repository.

Creating a VLAN Pool

To create a VLAN pool, perform the following steps.

Step 1 Choose **Service Inventory > Inventory and Connection Manager > Resource Pools**.

The Resource Pools window appears.

Step 2 Choose **VLAN** from the Pool Type drop-down list.

The Resource Pools - VLAN window appears.

Step 3 Click **Create**.

The Create VLAN Pool window appears, as shown in [Figure 2-17](#).

Figure 2-17 VLAN Pool

Step 4 In the VLAN Pool Start field, enter a valid value.

Step 5 In the VLAN Pool Size field, enter a valid value.

- Step 6** Choose an access domain by clicking **Select**.
The Select Access Domain window appears.
- Step 7** Choose an **Access Domain**.
- Step 8** Click **Select**.
The Create VLAN Pool window reappears.
- Step 9** Click **Save**.
The Resource Pools - VLAN window appears showing the VLAN Pool in the Repository.

**Note**

The VLAN pool does not supply a value for a second VLAN ID, when that feature is used for Q-in-Q matching. See the section [Notes on the VLAN ID and Second VLAN ID Attributes, page 6-10](#) for additional information about second VLAN ID.

Defining VPNs

During service deployment, ISC generates the Cisco IOS commands to configure the logical VPN relationships. At the beginning of the provisioning process, before creating a Service Policy, a VPN can be defined within ISC.

**Note**

It is also possible to specify VPN and VRF information in an independent VRF object, which is subsequently deployed to a PE device and then associated with an MPLS VPN link via an MPLS VPN service request. For details on using this feature, see [Chapter 3, “Independent VRF Management.”](#)

This section describes how to define MPLS VPNs and IP Multicast VPNs. It contains the following sections:

- [Creating an MPLS VPN, page 2-22](#)
- [Creating an IP Multicast VPN, page 2-26](#)
- [Enabling a Unique Route Distinguisher for a VPN, page 2-28](#)

Creating an MPLS VPN

At its simplest, a virtual private network (VPN) is a collection of sites that share the same routing table. A VPN is also a framework that provides private IP networking over a public infrastructure such as the Internet. In Cisco IP Solution Center (ISC), a VPN is a set of customer sites that are configured to communicate through a VPN service. A VPN is defined by a set of administrative policies.

A VPN is a network in which two sites can communicate over the provider’s network in a private manner; that is, no site outside the VPN can intercept their packets or inject new packets. The provider network is configured such that only one VPN’s packets can be transmitted through that VPN—that is, no data can come in or out of the VPN unless it is specifically configured to allow it. There is a physical connection from the provider edge network to the customer edge network, so authentication in the conventional sense is not required.

To create an MPLS VPN, perform the following steps.

-
- Step 1** Click the **Service Inventory** tab.
- Step 2** Choose **Inventory and Connection Manager**.
The Inventory and Connection Manager window appears.
- Step 3** From the Inventory and Connection Manager window, choose **VPNs**.
The VPNs window appears.
- Step 4** From the VPNs window, click **Create**.
The Create VPN window appears, as shown in [Figure 2-18](#).

Figure 2-18 Create VPN

Create VPN

Name* :

Customer* : Select

MPLS Attributes

Create Default CE Routing Community: Provider1

Enable Unique Route Distinguisher:

Enable Multicast:

Enable Auto Pick MDT Addresses:

Default MDT Address* : (a.b.c.d)

Data MDT Subnet: (a.b.c.d)

Data MDT Size:

Data MDT Threshold: (1 - 4294967 kilobits/sec)

Default PIM Mode: SPARSE_DENSE_MODE

MDT MTU: (576 - 18010)

Enable PIM SSM: DEFAULT

SSM List Name* :

Multicast Route Limit: (1 - 2147483647)

Enable Auto RP Listener:

Configure Static-RP:

PIM Static-RPs* : Showing 0 of 0 records Edit

#	Static-RP Unicast Address	Multicast-Group List Name	Override
Rows per page: <input type="text" value="10"/> Go to page: <input type="text" value="1"/> of 1 Go			

CE Routing Communities: Select
Remove

VPLS Attributes

Enable VPLS:

VPN ID: (1-2147483646)

Service Type: ERS

Topology: Full Mesh

Save Cancel

211613

Step 5 Name: Enter the name of the VPN.

Step 6 Customer: To choose the customer associated with this VPN:

- a. Click **Select**.
The Select Customer dialog box appears.
- b. From the list of customers, choose the appropriate customer, then click **Select**.
The Create VPN window reappears.

- Step 7 Create Default CE Routing Community:** To create a default CE routing community, check the **Create Default CE Routing Community** check box and choose a provider.
- Step 8 Enable Unique Route Distinguisher:** For coverage of this attribute see [Enabling a Unique Route Distinguisher for a VPN, page 2-28](#).
- Step 9 Enable Multicast:** To enable multicast for the VPN, see [Creating an IP Multicast VPN, page 2-26](#).
- Step 10 CE Routing Communities:** If you do not choose to enable the default CERC, you can choose a customized CERC that you have already created in ISC (see [Creating CE Routing Communities, page 2-32](#)).



Note You must specify a CERC if multicast is enabled.

- a. From the CE Routing Communities pane, click **Select**.
The Select CE Routing Communities dialog box appears.
- b. Check the check box for the CERC you want used for this VPN, then click **Select**.
You return to the Create VPN dialog box, where the new CERC selection appears, along with its hub route target (HRT) and spoke route target (SRT) values, as shown in [Figure 2-19](#).

Figure 2-19 New CERC Selected

MPLS Attributes	
Create Default CE Routing Community:	<input checked="" type="checkbox"/> PROV1
Enable Multicast:	<input checked="" type="checkbox"/>
Data MDT Size:	16
Data MDT Threshold:	0 (1 - 4294967 bits/sec)
CE Routing Communities:	<div style="border: 1px solid gray; padding: 5px;">CERC2: 100:604(HRT)/100:605(SRT)</div> <div style="text-align: right;"> <input type="button" value="Select"/> <input type="button" value="Remove"/> </div>
VPLS Attributes	
Enable VPLS:	<input type="checkbox"/>
Service Type:	ERS
Topology:	Full Mesh
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

- Step 11 Enable VPLS:** (Optional) Check this check box to enable VPLS.
- Step 12 Service Type:** (Optional) Choose the VPLS service type from the drop-down menu: **ERS** (Ethernet Relay Service) or **EWS** (Ethernet Wire Service).
- Step 13 Topology:** (Optional) Choose the VPLS topology from the drop-down menu: **Full Mesh** (each CE will have direct connections to every other CE) or **Hub and Spoke** (only the Hub CE has connection to each Spoke CE and the Spoke CEs do not have direct connection to each other).
- Step 14** When satisfied with the settings for this VPN, click **Save**.

You have successfully created a VPN, as shown in the Status display in the lower left corner of the VPNs dialog box.

Creating an IP Multicast VPN

An IP address that starts with the binary prefix 1110 is identified as a *multicast group address*. There can be more than one sender and receiver at any time for a given multicast group address. The senders send their data by setting the group address as the destination IP address. It is the responsibility of the network to deliver this data to all the receivers in the network who are listening to that group address.


Note

Before you can create a VPN with multicast enabled, you must define one or more multicast resource pools. See [Creating a Multicast Pool, page 2-16](#), for further information.


Note

If the multicast VPN is used in a service request for IPv4 on a device running IOS XR, not all of the multicast attributes in the Create VPN window are supported. This is because there is not a one-to-one mapping of IOS multicast commands to IOS XR commands. These exceptions are noted in the following steps. For a comparison of multicast routing commands in IOS and IOS XR, see [Multicast Routing on IOS XR Devices, page 4-6](#).


Note

Multicast VRF deployments are supported only for IPv4 deployments. They are not supported for either IPv6 or IPv4+IPv6 modes. For more information about VRF object support in ISC, see [Chapter 3, “Independent VRF Management.”](#)

To create an IP Multicast VPN, follow the procedure described in [Creating an MPLS VPN, page 2-22](#) to the place where you can enable multicast for the VPN, then perform the following steps.

-
- Step 1** To enable multicast for the VPN, check **Enable Multicast**.
- The current window refreshes with additional fields becoming active.
- Step 2** For MDT (Multicast Distribution Tree) addresses, either accept the default (check box already checked) to enable the auto pick function, or uncheck the auto pick check box, then enter values in the next two fields:
- Default MDT Address
 - Data MDT Subnet
- Step 3** From the drop-down list, choose a value for Data MDT Size.
- Step 4** In the next field, enter a valid value for Data MDT Threshold (1 - 4294967 kilobits/sec).
- Step 5** For Default PIM (Protocol Independent Multicast) Mode, choose a mode from the drop-down list:
- SPARSE_MODE
 - SPARSE_DENSE_MODE


Tip

Multicast routing architecture allows the addition of IP multicast routing on existing IP networks. PIM is an independent unicast routing protocol. It can be operated in two modes: dense and sparse.



Note For IOS XR devices, when SPARSE_DENSE_MODE is chosen, no configlet will be generated. Sparse-dense mode is not supported by IOS XR, only sparse mode (default) and bidirectional mode. For IOS XR devices, sparse mode is running by default when multicast routing is enabled on an interface. Hence, no configlet will be generated for sparse mode either.

Step 6 In the next field, enter a valid value for MDT MTU (Maximum Transmission Unit).



Note The ranges for IOS and IOS XR devices for this attribute are different. The range for IOS devices is from 576 to 18010, and for IOS XR devices it is from 1401 to 65535. Device type validations are done during service request creation when it is known what type of device the multicast VPN will be deployed on.

Step 7 To enable PIM SSM (Source Specific Multicast), check the associated check box.

When you check the check box:

- a. The associated drop-down list goes active with the DEFAULT enumeration populated as the SSM default. This will create the following CLI: **ip pim vrf vrfName ssm default**.



Note For IOS XR devices, when DEFAULT is chosen, no configlet will be generated because this command is running by default on IOS XR devices, using the standard SSM range 232.0.0.0/8.

- b. If you would like to associate an access-list number, or a named access-list, with SSM configuration, choose the RANGE enumeration from the SSM drop-down list instead of DEFAULT. This will create the following CLI: **ip pim vrf vrfName ssm range {ACL# | named-ACL-name}**.

Step 8 If you choose RANGE in the previous step, then the next field goes active for you to enter Access-list number or Access-list name.

Step 9 In the next field enter a valid value for the Multicast Route Limit (1 - 2147483647).



Note For IOS XR devices, no configlet is generated for this attribute. The command to set the route limit per VRF is not supported on IOS XR devices.

Step 10 To enable the auto RP (Rendezvous Point) listener function, check the associated check box.



Note For IOS XR devices, no configlet is generated for this attribute. By default, this feature is running on IOS XR devices.

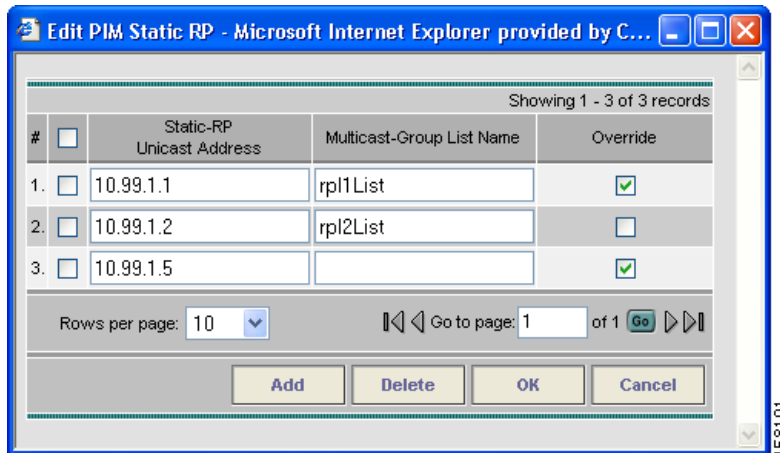
Step 11 To configure Static RPs, check the associated check box.

When you check this, the Edit option for PIM Static RPs goes active.

Step 12 To edit or add PIM Static RPs, click **Edit**.

The Edit PIM Static RPs window appears, as shown in [Figure 2-20](#).

Figure 2-20 Edit PIM Static RPs



Step 13 Complete all applicable fields in the Edit PIM Static RP window, then click **OK**.

The data now appears in the main Create VPN window.

Step 14 To save your changes and add this Multicast VPN to you system, at the bottom of the window, click **Save**.

Enabling a Unique Route Distinguisher for a VPN



Note

In ISC 5.1, enabling unique route distinguishers is only supported for IOS devices. It is not supported for IOS XR devices.

Support for multipath load sharing requires unique route distinguishers (RDs) for each PE router for a VPN (VRF). This is to prevent the same RDs from being allocated to different customers. This allows the use of the same RD for the same VRF. That is, all sites in the PE can have the same unique RD. The unique RD feature is optional. It is enabled at both a global VPN level or a service request level. To enable the unique RD per PE for a VPN, the Create VPN window contains the attribute **Enable Unique Route Distinguisher** field.

Each VPN deployed through ISC for which **Enable Unique Route Distinguisher** has been selected is marked as a multipath VPN. This ensures a unique RD allocation for each VRF on each PE. Enabling multipath for an already deployed VPN creates new VRFs on all the PEs of the VPN and assigns a unique RD. When **Enable Unique Route Distinguisher** is selected for the VPN, the **Allocate New Route Distinguisher** and **VRF and RD Overwrite** attributes will be disabled when setting up a policy or service request that uses this VPN.

To use the unique RD feature, perform the following steps.

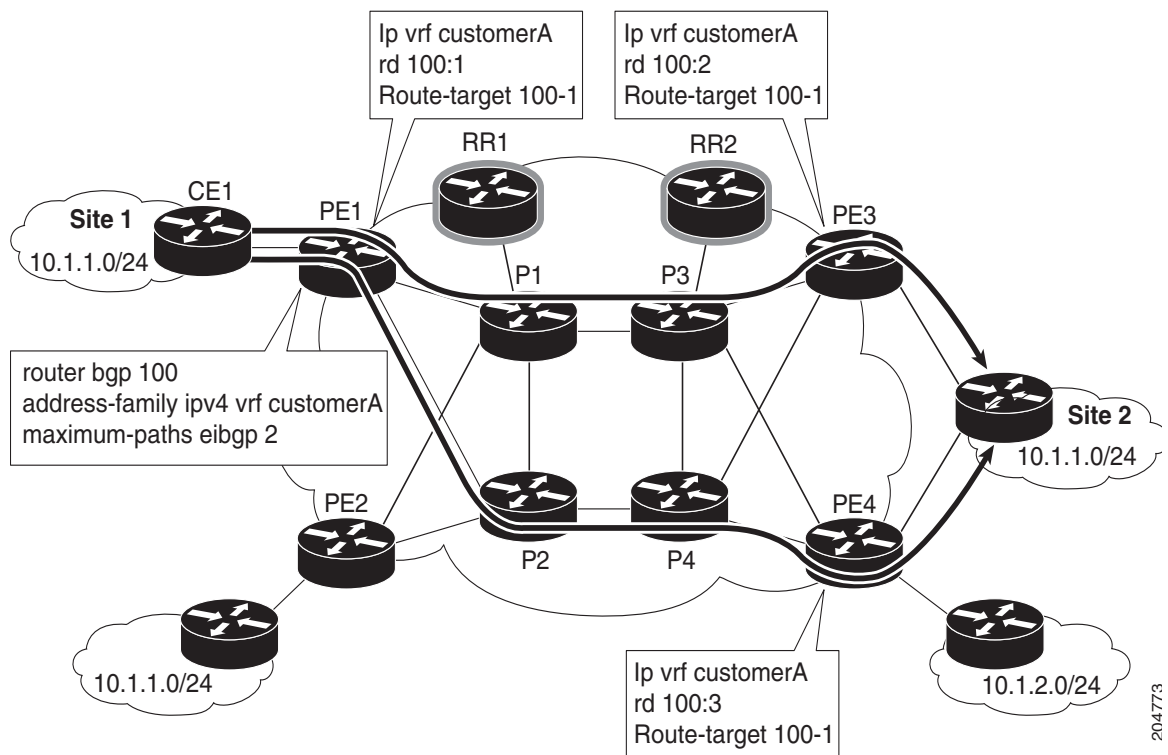
-
- Step 1** When creating a VPN, check the **Enable Unique Route Distinguisher** check box.
- Step 2** When subsequently creating a service policy and/or service request, select the VPN in the VRF and VPN Membership window.
- The Unique Route Distinguisher **field** appears.
- Step 3** If the unique RD allocation functionality is required, check the **Unique Route Distinguisher** check box.
-

For additional information on how this feature is used with MPLS VPN policies and service requests, see [Defining VRF and VPN Information](#), page 5-29.

Provisioning MPLS Service Requests Using Unique Route Distinguisher

The unique route distinguisher (RD) feature is used to implement multipath load balancing. Multihomed CEs often require load balancing across multiple available paths. In a full-mesh BGP environment, PEs receive all the available paths to a given prefix, and load balancing can easily be achieved. However, when route reflectors are present in the service provider core, PE routers receive only one route, even if multiple paths exist, and load balancing does not occur. To achieve load balancing, the service provider needs to implement unique RD values for the customer VPN on each PE router. In addition, eIBGP configuration with the desired number of paths (across which load balancing is desired) needs to be enabled in the service provider environment. [Figure 2-21](#) illustrates a load balancing example.

Figure 2-21 Load Balancing Using Different RDs



204773

The support for multipath load sharing requires unique RDs for each PE router for a VPN (VRF). This is to prevent the same RDs from being allocated to different customers. This allows the use of the same RD for the same VRF. That is, all sites in the PE can have the same unique RD. The unique RD feature is optional. You can specify its use at both the policy or service request level.

It is enabled at both a global VPN level or a service request level.

ISC supports BGP multipath load sharing through fields and options in the ISC GUI. The following steps provide an overview of how to do this.

- Step 1** When creating a VPN, check the **Enable Unique Route Distinguisher** check box in the Create VPN window, as shown in [Figure 2-22](#).

Figure 2-22 Enabling Unique RD in Create VPN

Create VPN	
Name *	vpn_1
Customer *	<input type="text"/> <input type="button" value="Select"/>
MPLS Attributes	
Create Default CE Routing Community:	<input type="checkbox"/> Provider1 ▾
Enable Unique Route Distinguisher:	<input checked="" type="checkbox"/>
Enable Multicast: ⓘ	<input type="checkbox"/>

For some additional coverage of this, see [Enabling a Unique Route Distinguisher for a VPN](#), page 2-28.

- Step 2** When setting the attributes in the policy (MPLS Policy Editor - VRF and VPN Membership window) or service request (MPLS Link Attribute Editor - VRF and VPN window), use the **BGP Multipath Load Sharing** check box to enable or disable BGP multipath load sharing.

Enabling BGP multipath load sharing by checking the check box causes additional attributes to appear in the GUI. For detailed coverage of these attributes and how to set them, see [BGP Multipath Load Sharing and Maximum Path Configuration](#), page 5-32.

- Step 3** When creating a service request based on this policy, check the **Unique Route Distinguisher** check box in the MPLS Link Attribute Editor - VRF and VPN window, as shown in [Figure 2-23](#).

Figure 2-23 Enabling Unique Route Distinguisher in a Service Request

MPLS Link Attribute Editor - VRF and VPN

Attribute	Value				
VRF Information					
Use VRF Object:	<input type="checkbox"/>				
Export Map:	<input type="text"/>				
Import Map:	<input type="text"/>				
Maximum Routes:	<input type="text"/> (1-4294967295)				
Maximum Route Threshold *:	<input type="text"/> 80 (1-100)				
VRF Description:	<input type="text"/>				
BGP Multipath Load Sharing:	<input type="checkbox"/>				
Unique Route Distinguisher:	<input checked="" type="checkbox"/>				
Allocate New Route Distinguisher:	<input type="checkbox"/>				
VRF And RD Overwrite:	<input type="checkbox"/>				
VPN Selection					
PE VPN Membership *:					
Select	Customer	VPN	Provider	CERC	Is Hub
<input type="checkbox"/>	Customer1	vpn_3	Provider1	CERC_1	<input checked="" type="checkbox"/>
					<input type="button" value="Add"/> <input type="button" value="Delete"/>

Note: * - Required Field

204775

**Note**

The Unique Route Distinguisher attribute is dynamic and only shows up in the GUI if a VPN with unique RD enabled is selected.

Step 4

Complete the service request creation, and save the service request.

Use Cases for Using Unique RD

The following use cases demonstrate the behavior of unique RD feature.

Use case details:

- The default values of the VPN/VRF are:

```
ip vrf V24:unique2
rd 1:33
route-target import 1:14
route-target import 1:15
route-target export 1:14
```

- Service requests are created using PEs and enabling or disabling the Unique RD attribute during service request creation, as shown in [Table 2-1](#).
- The outcomes for various cases are described in the Results column of the table.

Table 2-1 Unique RD Use Cases

SR #	PE	Unique RD	VRF:RD	Results
1	pe1	False	V24:33	ISC uses the default <i>vrfName:RD</i> , because this is the first time this PE has been configured with this <i>vrfName:RD</i> name.
2	pe2	False	V24:33	ISC uses the default <i>vrfName:RD</i> .
3	pe3	True	V25:34	ISC creates a new <i>vrfName:RD</i> , because Unique RD is true, and it is on a different PE. This PE (pe3) did not have this <i>vrfName:RD</i> configured.
4	pe3	True	V25:34	ISC uses the <i>vrfName:RD</i> from SR #3, because the new RD is already present on the PE router.
5	pe2	True	V26:35	ISC creates a new <i>vrfName:RD</i> , because this is the first time Unique RD is selected as true, even though a VRF of V24:33 was already configured in SR #2.
6	pe1	True	V27:36	ISC creates a new <i>vrfName:RD</i> , because this is the first time Unique RD is selected as true on this PE, even though a VRF of V24:33 was already configured in SR #1.
7	pe1	False	V24:33	ISC uses the default <i>vrfName:RD</i> , as in SR #1.
8	pe3	False	V24:33	ISC uses the default <i>vrfName:RD</i> , as in SR #1.
9	pe3	True	V25:34	ISC uses the newly created <i>vrfName:RD</i> in SR #4, because it already created a new <i>vrfName:RD</i> for this PE.
10	pe2	True	V26:35	ISC uses the newly created <i>vrfName:RD</i> in SR #5, because it already create a new <i>vrfName:RD</i> for this PE.
11	pe1	True	V27:36	ISC uses the newly create <i>vrfName:RD</i> in SR #6, because it already create a new <i>vrfName:RD</i> for this PE.

Creating CE Routing Communities

CE Routing Communities (CERCs) are the means by which ISC handles the Route Targets (RT) transparently from the users, and it can help the service providers to easily implement various kinds of VPN topology. When you create a VPN, the ISC software creates one default CE routing community (CERC) for you. But if your network topology and configuration require customized CERC definitions, you can define CERCs customized for your network.



Tip

Customized CERCs should be defined only in consultation with the VPN network administrator.

To build complex topologies, it is necessary to break down the required connectivity between CEs into groups, where each group is either fully meshed, or has a hub-and-spoke pattern. A CE can be in more than one group at a time, so long as each group has one of the two basic configuration patterns.

Each subgroup in the VPN needs its own CERC. Any CE that is only in one group just joins the corresponding CERC (as a spoke if necessary). If a CE is in more than one group, then you can use the Advanced Setup choice during provisioning to add the CE to all the relevant groups in one service request. Given this information, ISC does the rest, assigning route target values and VRF tables to arrange the precise connectivity the customer requires.

To define a new CERC, perform the following steps.

-
- Step 1** Click the **Service Inventory** tab.
- Step 2** Choose **Inventory and Connection Manager**.
The Inventory and Connection Manager window appears.
- Step 3** Choose **CE Routing Communities**.
The CE Routing Communities window appears.
- Step 4** Click **Create**.
The Create CE Routing Community window appears, as shown in [Figure 2-24](#).

Figure 2-24 Defining a New CE Routing Community

- Step 5** Complete the CERC fields as required for the VPN:
- Provider: To specify the service provider associated with this CERC, click **Select**.
The Select Provider dialog box appears.
 - Choose the name of the service provider, then click **Select**.
 - Name: Enter the name of the CERC.
 - CERC Type: Specify the CERC type: Hub and Spoke or Fully Meshed.
 - Auto-Pick Route Target Values: Choose to either let ISC automatically set the route target (RT) values or set the RT values manually.
By default, the **Auto-pick route target values** check box is checked. If you uncheck the check box, you can enter the Route Target values manually.



Note If you choose to bypass the **Auto-pick route target values** option and set the route target (RT) values manually, the RT values cannot be edited after they have been defined in the Cisco IP Solution Center software.

Step 6 When you have finished entering the information in the Create CE Routing Community dialog box, click **Save**.
