HPSA - VPN SVP 6.0

User's Guide
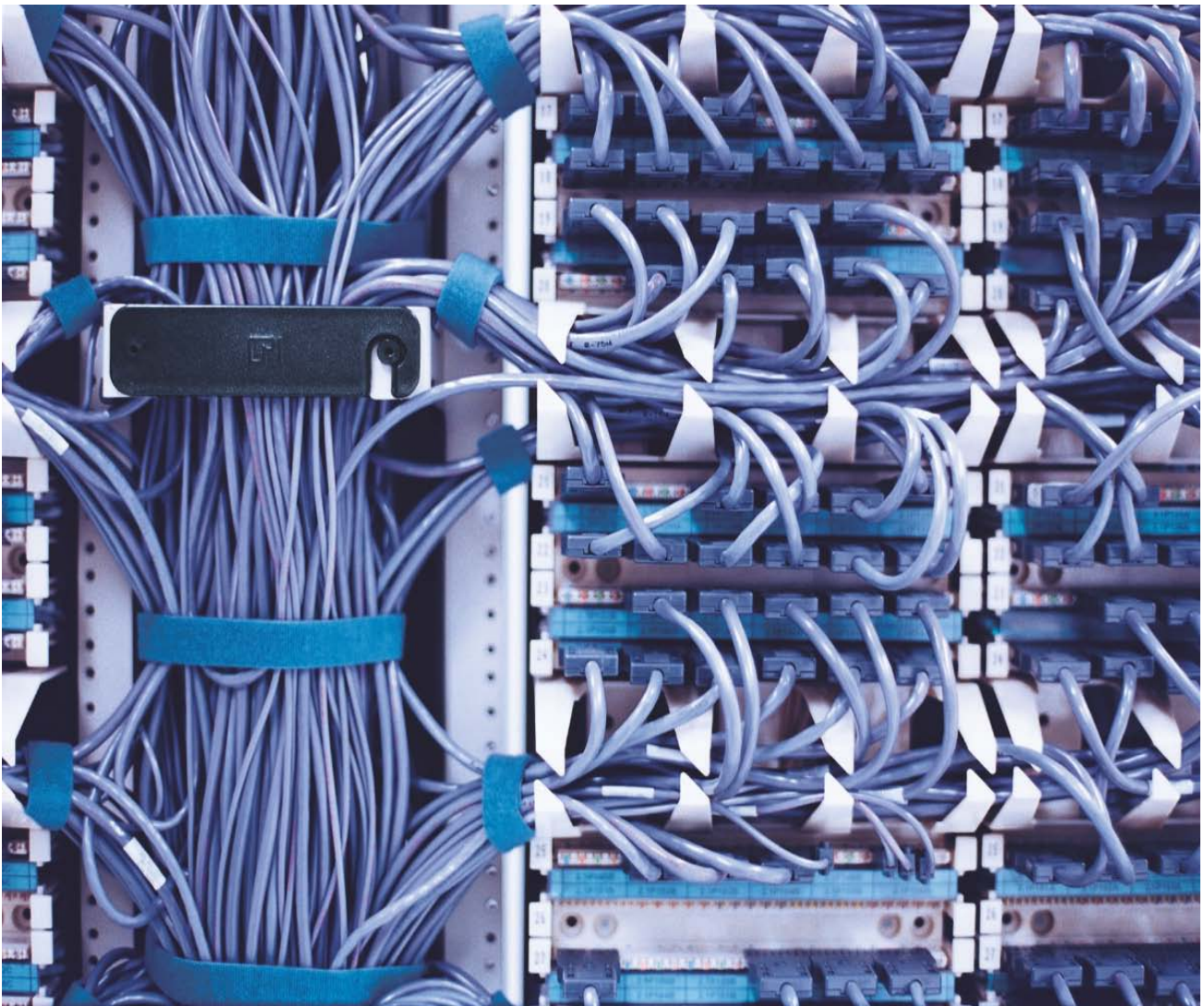
Reference number: p180-pd000101

Edition: May 2012

Contents

1 Introduction

1-1 In this Guide

This document is the User's Guide to the HP Service Activator (HPSA) based VPN Solution, which is a solution suite managing MPLS based VPN services, from order entry to activation in the network.

The objective of this guide is to offer assistance to Operators that uses or are going to use the Service Activator VPN Solution Pack (VPN_SVP) for their network service provisioning work.

It is assumed that Operators have basic knowledge of Service Activator and extensive knowledge of Layer 2 and Layer 3 VPN MPLS technology.

You may find further information about setup, initial configuration and other administrative procedures of VPN_SVP in [*ADM*].

1-2 Manual Organization

Each chapter covers different functionality of the VPN_SVP. Only the main functionality will be described and no emphasis has been put on the features of the HPSA core product.

Below is a brief description of the chapters in this document.

Chapter 2 introduces the VPN_SVP and its features

Chapter 3 describes the basic set-up of the HPSA inventory parts (such as locations, networks, routers).

Chapter 4 focuses on customer records management in CRM Portal. It explains how new customers are entered, how customer records are searched for or are deleted.

Chapter 5 explains how a Layer 2 VPN (VPLS) service is activated. The CRM operator enters the customer order in CRM Portal and forwards the request to Service Activator for the Network operator to complete activation tasks.

Chapter 6 explains how a Layer 2 VPWS service is activated. The CRM operator enters the customer order in CRM Portal and forwards the request to Service Activator for the Network operator to complete activation tasks.

Chapter 7 guides you through activating Layer 3 VPN services. The CRM operator enters the customer order in CRM Portal and forwards it to Service Activator for the Network operator to complete the activation tasks.

Chapter 8 describes a set of additional facilities not related to specific service types.

Chapter 9 explains how to use the Reporting tool to extract information from the Inventory database.

Chapter 10 guides you through Error and Diagnostic handling of failed service requests. The tools available to the network operator are presented and explained.

Chapter 11 addresses Back-up and Restore processes

Chapter 12 describes the integration of HPSA and HP NNMi.

Chapter 13 describes the integration of HPSA and HP NA.

1-3 Install Location Descriptors

The following names are used to define install locations throughout this guide.

Table 1 Install Location Descriptors

Descriptor	What the Descriptor Represents
$JBOSS_DEPLOY	The install location of the JBoss applications. The UNIX location is: /opt/HP/jboss/server/default/deploy The Windows location is: *<install drive>*:\HP\jboss\server\default\deploy
$SOLUTION	The install location of the VPN_SVP solution. The UNIX location is: /opt/OV/ServiceActivator/solutions/SAVPN The Windows location is: *<install drive>*:\HP\OpenView\ServiceActivator\solutions\SAVPN

1-4 References

List of References

Reference	Document Title	File Name
ADM	HPSA - VPN SVP 6.0 Administrator's Guide	AdminGuide.pdf*
SDG	HPSA - VPN SVP 6.0 Service Discovery Guide	SDGuide.pdf*
REL	HPSA – VPN SVP 6.0 Release Notes	ReleaseNotes.pdf*
INTRO	HP Service Activator User's and Administrator's Guide. Edition V60	HPSA-User.pdf**
INTEGRATE	HP Service Activator System Integrator's Overview. Edition V60-1A	Overview.pdf**
NA_USR	HP Network Automation User's Guide	User_guide.pdf[+]

NOTE1: * Documents available in the HPSA VPNSVP solution docs folder.

NOTE2: ** Documents available in the HP Service Activator docs folder.

NOTE3: [+] Documents available in the HP Network Automation docs folder.

2 Introduction to VPN Solution Pack

The HP Service Activator VPN Solution Pack (or VPN_SVP) implements a multi vendor VPN provisioning solution which automates common repetitive task and which provides a convenient collection of tools to ease the daily work of a Service Provider.

2-1 What is the VPN_SVP?

The VPN_SVP software extends the value and benefits of the HP Service Activator framework.

The objective of the VPN_SVP is to:

- Provide an easy-to-use platform for VPN provisioning and management which enhances the effectiveness of the provider's operations and lowers the risk of configuration errors and service outages
- Reduce time to deployment through pre-implemented workflows and configuration templates
- Facilitate integration with the multi vendor equipment as well as other support systems
- Include MPLS VPN Service Management expertise, configuration recommendations and best practices
- Includes a pan-optic network management integration foundation, currently towards HP Network Node Manager (NNMi) and HP Network Automation (NA) for network discovery, data load, VPN service integrity checks and GUI cross-launch.
- Provide an operational foundation for a solution that can easily be customized and extended to map specific customer contexts
- Include a multi-vendor catalogue of solutions and components that constantly develop in line with new services

The VPN_SVP normally requires some customization and extensions to provide the precise services and facilities requested by a particular customer. The flexibility and openness of the HPSA framework and of VPN_SVP provides an ideal environment for customer specific modifications and extensions.

2-2 Content of VPN_SVP

The VPN_SVP contains several components in addition to the standard HPSA features to support the operational procedures of VPN Service Providers.

- A general service request/response interface (North Bound Interface, NBI) for integration with Order Management systems or other operations support systems.
- A simple CRM Portal GUI, which provides an easy-to-use interface for Customer Order related personnel to manage the Customer ordered services to be provisioned or activated in the Provider's network. Displays a summary of the states of various services requested by the various customers.
- An Inventory repository which maintains Service, Equipment and Configuration related objects and parameters
- An Inventory GUI which provides an easy-to-use Network Operator interface for viewing Services and their related resources as well as configuring and creating resources and parameters necessary for the Service Provider's operations.
- A set of device and vendor independent HPSA Workflows which implements the service creation, modifications and deletion operations on PE and CE devices

- A service agnostic set of device and vendor independent HPSA Workflows which implements creation of service attachments via an L2 switch based Access Network.

- A set of corresponding vendor, device and OS dependent activation templates, which implements the device specific configuration commands which are necessary for configuring the requested services and/or modifications and deletions.

- Role based GUIs and Workflows which allows association of views and operations to the role of the operator.

- NNM Liaison component that provides integration between the service fulfillment (HPSA) and service assurance (HP NNMi) products to provide service information into the assurance application and equipment and topology load into the fulfillment application.

- NA Liaison component that guarantees the service integrity between the network and the fulfillment application.

- Network interface upload tool that provides automatic creation of NE related inventory elements, such as ports, interfaces and controllers from information uploaded from the NE.

- A Service Discovery tool that allows VPN_SVP to discover configured services from the network device configurations. This may be used to commence VPN_SVP in an already running environment.

- A Work-order tool, which provides CE management via manual work orders. Work-orders are e.g. generated in cases where either the CE is not present in the network and connectivity cannot be established or the detailed configuration commands are not (yet) implemented in activation templates.

- A work-order distribution component that allows Work-orders to be automatically send by e.g. email to 3rd-party clients that are responsible for setting up managed CE devices, or to the contact person of the customer in case of an unmanaged CE device.

- A Reporting Tool that provides information about the services and resources managed by VPN_SVP. This information augments the Inventory information view, in a way which is not readily available in the Inventory GUI.

- An Error/Diagnostic Handler that allows the operator to analyze, diagnose and possibly resubmit failed service requests. Supports resource retention or reselection as well as skip activation mode.

- A Delayed Activation component that allows requests that fails due to temporary connectivity problems between the NOC and the NEs to be retried automatically.

- An Interface Recovery tool, which allows the operator to move all existing services to an available replacement port in case a physical port e.g. burns out.

- An xml based Inventory importer/exporter tool which supports backup, data migration and data load of the complete Inventory database of VPN_SVP.

- A generic configuration Backup tool which allows for manual and automatic periodic backup and restore of Network Element (PE and CE) configurations as well as audit compare function which helps in validation and verification of equipment configurations. Supports any transfer protocol that the vendor specific devices may support.

- The Audit tool of HPSA is used to store historic records (audit trails) in the database for each activation/modification performed on any NE. Combined with the Backup Tool this may be used to recover the complete configuration of a failed NE.

Figure 2-1 VPN Solution components augmenting HP Service Activator core components
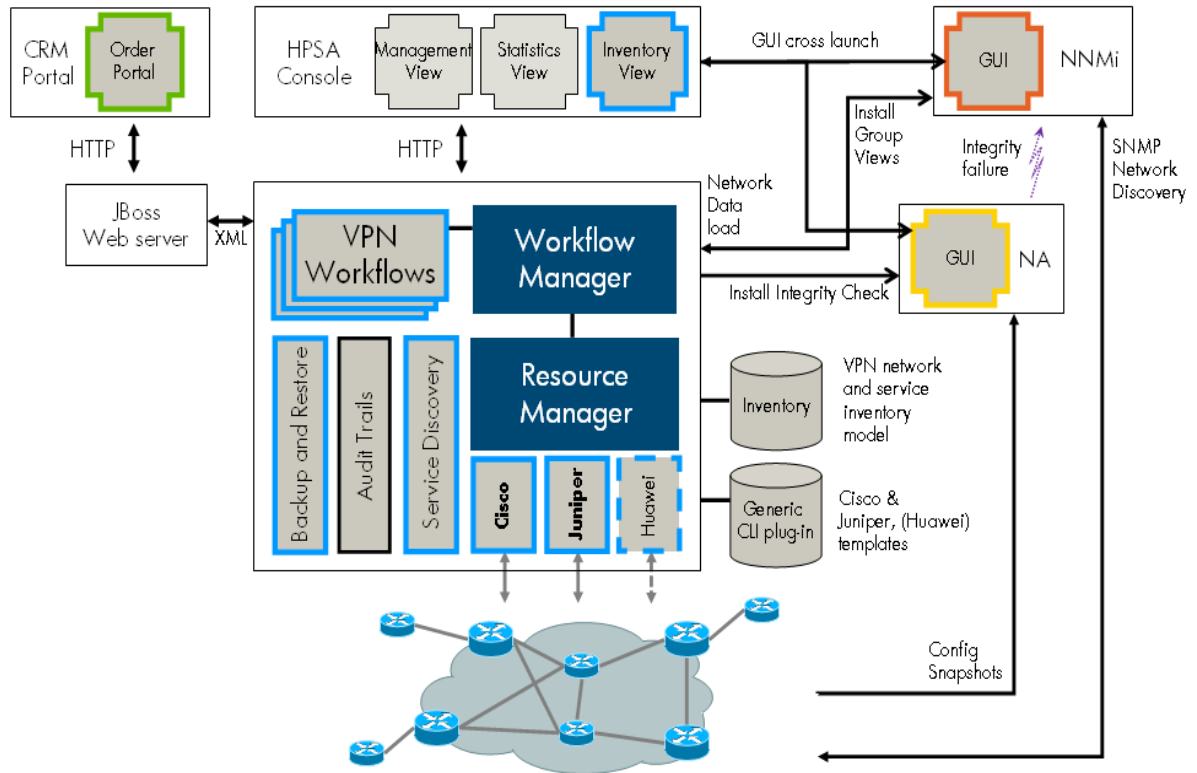
2-3 Services of VPN_SVP

The VPN_SVP automates or simplifies the major part of the following service provisioning tasks:

- A simple CRM Portal and GUI, which provides and easy-to-use interface for Customer Order related personnel to request the services ordered by the Customer to be provisioned or activated in the Provider's network using the NBI of VPN/HPSA.

- Creation and deletion of IPv4 or IPv6 based L3 VPN service.
  This activity does not induce any configuration of the NEs. The VPN object serves as a container for VPN wide attributes, default values and the site services. VPN topologies Fully-meshed and Hub & Spoke are supported.

- Layer 3 multicast is supported (PIM sparse and sparse-dense mode)

- Addition and removal of IPv4 or IPv6 Layer 3 VPN Site service. This includes allocation and reservation of the various Layer 3 VPN and Site specific resources and the configuration of the PE and optionally CE routers:
  - PE-CE connection routing protocol:
    - RIP
    - OSPF
    - eBGP
    - Static routes
  - QoS, and for a Managed CE optionally CE based QoS
    - Rate Limit (aggregated BW)
    - Up to 8 CoS, percentage allocation bandwidth
  - Classification based on:
    - DSCP

- – IPAddr, TCP/UDP port
  - ○ Automatic addition of AdminVPN Spoke configuration of the PE VRF for Managed CEs
  - ○ Selection among Multiple PE-CE link address pools for the allocation of PE-CE connection addresses
  - ○ Address pool with /31 network mask are supported
  - ○ Encapsulation of attachment circuits. The following types are supported:
    - – Serial: HDLC, PPP and Frame Relay including selection of DLCI
    - – Ethernet: None or 802.1Q including selection of VLAN Id
- Creation and maintenance of IPv4 and IPv6 address pools that support IPv4 as well as IPv6 based L3 services.
- Protection configuration/multi-homing of Layer 3 Site services. This includes configuration of multiple (dual) attachment circuits connecting a Layer 3 Site CE to different PEs in the provider network. This requires that the PE-CE routing protocol is eBGP.
- Modification of Layer 3 Site services. This includes modification of the following Site specific (shared) parameters:
  - ○ Connectivity Type (Full Mesh, Hub, Spoke)
  - ○ Multicast (Rendezvous Point, Rate-limit, CoS)

  and the following attachment circuit specific parameters:
  - ○ Add/Remove Static Routes
  - ○ Rate Limit (aggregated BW)
  - ○ QoS
- Join/Leave VPN. These operations allow a site to become a member of multiple VPNs. The VRF is modified to include the RC of the VPN to join. Likewise, Leave removes the associated RC. This may be used to implement e.g. extranet and Intranet access VPNs.
- Support the setup an construction of the providers network infra structure based on multiple AS numbers (multi-AS-backbone), and automates the creation and deletion of ASBR links across multiple AS when services are created/deleted.
- Configuring attachment of L3 services via a generic L2 switched Access Network component. Manages allocation and configuration of service specific Vlan ids (1:1 mapping) on access ports and adding these to the trunk ports in the access network.
- Provides optionally addition of VRRP configuration for L3 services that are attached via L2 access network to multiple PE routers to provide a standard based PE router redundancy features.
- Creation and Deletion of Layer 2 VPN service (Virtual Private LAN Service or VPLS). This activity does not induce any configuration of the NEs. The VPN object serves as a container for VPN wide attributes, default values and the site services
- Addition and removal of Layer 2 VPN Site service. This includes allocation and reservation of the various Layer 2 and Site specific resources. Both explicit mesh configuration mode and BGP auto-discovery modes are supported
  - ○ The following UNI Types are supported:
    - – Ethernet Port
    - – Ethernet PortVlan
  - ○ QoS includes:
    - – Rate limit
    - – Up to 8 CoS
    - – Classification based on 802.1Q p-bits
- Modification of Layer 2 Site services. This includes:

- ○ Rate Limit (aggregated BW)
- ○ QoS
- Creation and deletion of Layer 2 VPWS (Virtual Private Wire Service or point-to-point) services of Port, Port-VLAN, Frame Relay and PPP types. The following combinations of UNI types are supported:
  - ○ Eth Port↔Eth Port
  - ○ Eth PortVlan↔Eth PortVlan, FR, PPP
  - ○ FR↔Eth PortVlan, FR, PPP
  - ○ PPP↔Eth PortVlan, FR, PPP
- QoS includes:
  - ○ Rate Limit
  - ○ CoS (1 out of 8)
- Modification of Layer 2 VPWS services. This includes:
  - ○ Rate Limit
- Configuring attachments of L2 services via a generic L2 switched Access Network component. Manages allocation and configuration of service specific Vlan ids (1:1 mapping) on access ports and adding these to the trunk ports in the access network.
- Supports Region specific Vlan id and DLCI allocation schemes.
- Allows addition of multiple service types to an existing Site service (service multiplexing). If a site's existing attachment type is Vlan based (and not port based) multiple services may be associated a single site. This includes a mix of L3 and L2 services.
- A strategic Traffic Engineering component that builds a full mesh of LSPs between the PE routers hosting VPN sites. This involves automatic creation, deletion and modifications of LSPs according to the service requests and supports automatic or manual LSP bandwidth modification.
- Timed activation of Layer 2 VPLS, Layer 2 VPWS and Layer 3 VPN Site operations such as creation and modification. The Schedule specification may include:
  - ○ Start Time: The time when the requested services is to be activated
  - ○ End Time: The (optional) time when the service is to be de-activated
  - ○ Recurrence: Daily | Weekly | Monthly. Only modify Rate limit is currently supported as recurrent.
- Disabling/Enabling of Services. This allows a Site service or a complete VPN service to be stopped without releasing any allocated resources. Hence, these services may easily be re-enabled.
- Generic failure, retry and diagnostic management. This includes a common interface from where access to specific service provisioning information is made available:
  - ○ Request message, activation dialog, device communication log
  - ○ Option to re-try with our without resource retention or fail the service request.
  - ○ Temporary connectivity failures to the NEs are retried automatically by the delayed activation component
- Service recovery due to equipment failures. This includes an automated interface recovery tool, which allows the operator to migrate all services configured on a specific port is to a selected replacement port.
- Discovery of Services from network elements. Analyzes the configuration files of the NEs and discovers the configured services. This information may be reconciled by the operator before committing these into Inventory. For more information, see [*SDG*].

- NNM Liaison component that provides integration between the service fulfillment (HPSA) and service assurance (HP NNMi) products to provide service information into the assurance application and equipment and topology load into the fulfillment application.
- NA Liaison component that guarantees the service integrity between the network and the fulfillment application.
- In relation to MEF's (Metro Ethernet Forum's) Carrier Ethernet service specification, the VPN_SVP implements the services as indicated in **Table 2-2** below

Table 2-2 MEF Service Types

MEF Service Type	Port-based		Vlan-based		VPN/CE solution service name
E-LAN	EP-LAN	√	EVP-LAN	√	L2VPN (VPLS)
E-Line	EPL	√	EVPL	√	L2VPWS
E-Tree	EP-Tree	÷	EVP-Tree	÷	L2VPMS - Not yet supported

2-4 Activation Process of VPN_SVP

The VPN_SVP is structured around two web portals as illustrated in the **Figure 2-2** below. Each portal maintains its own process but the two are interrelated to each other via the exchange of service request and response messages via the NBI.

2-4-1 CRM Portal

It is assumed that the operators of CRM portal (or some other Order Management System) may be personnel different than the operators of the HPSA Portal. The CRM operators do not need any detailed knowledge about the network infrastructure and technologies but must design the customer related aspects of the services.

In the CRM Portal, the customer related aspects of the service activation process is maintained, i.e. creating, updating and possibly deleting customer records as well as advanced search facilities to locate a specific customer record among many.

The service life cycle is managed via the CRM portal. This includes associating services to the customer, designing the service order and it's specific parameters based on the customer's requirements, submitting the completed service orders for activation by Service Activator.

The services that have been associated customers may further be managed from the CRM Portal by Modify requests and eventually the services may be removed as well.

The state of the (optionally scheduled) service activation requests submitted to Service Activator is received from HPSA and maintained in the service views of the CRM Portal.

2-4-2 HPSA Portal

The HPSA portal operator must know the details of the provider network infrastructure and the technologies available, as in the Service Activator (HPSA) Portal the more resource facing aspects of the process is maintained. This includes allocation of network resources, e.g. devices and interfaces, by the network operator and e.g. automatic allocation of IP addresses and optionally Vlan ids.

Initially, the received service requests (orders) will automatically be validated in the HPSA to assure that the request is not contradicting constraints on existing service types, etc.

The creation of a site service may require the network operator to select the attachment point of the service, i.e. the router/switch and interface that the customer's site gets connected to. This is requested via an interaction form (AskFor) that automatically pops-up when required.
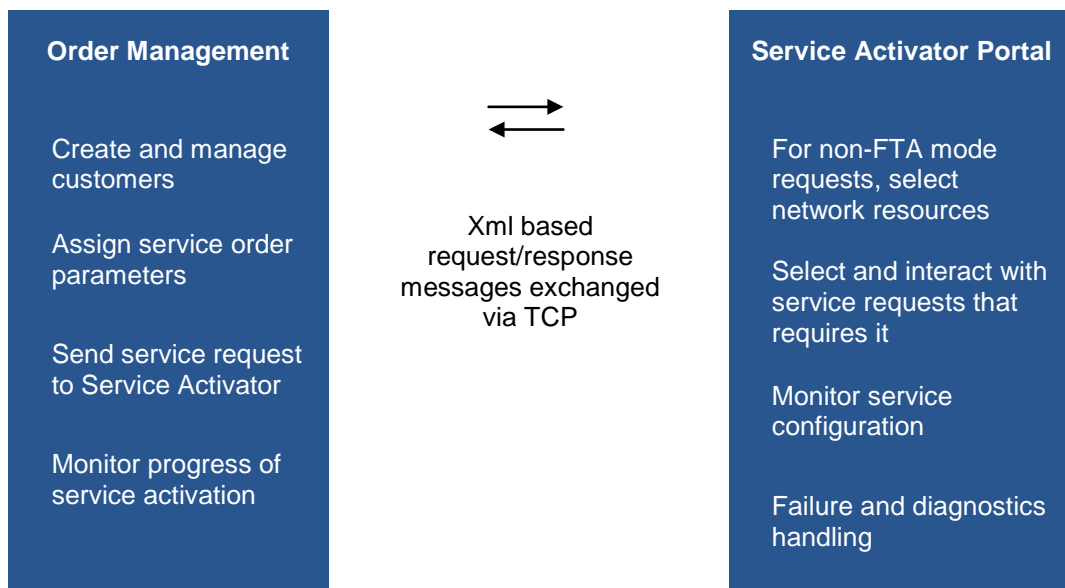
Optionally, the request may be of Flow-through type where the Order Management System specifies the required attachment point of the service and includes this in the request message. In Flow-through Activation (FTA) mode no interactions are required at activation time on VPN/HPSA.But often a received service request will anyway not require any interaction from network operators and will execute as a flow-through process on HPSA, e.g. when it is a modification of an existing service or any other operation that re-uses the already assigned resources.

For any operation, the progress and status will (optionally) be reported back to the CRM Portal (or some other north-bound order management system) to keep its state synchronized as mentioned above.

In cases of service activation failures, these may first be analyzed and diagnosed via the HPSA Portal's generic Error-Handler feature. This provides access to some of the information that is otherwise difficult to collect like a trace of the actual device dialog. Other information valuable for the diagnostic process is available via the standard HPSA GUIs. If the cause may be identified and even repaired, the request may be re-submitted from HPSA Portal. Otherwise, the request may be failed, optionally annotated with an operator entered description, and the responsibility of the process returns to the CRM Portal.

Failed FTA requests will return control to the Order Management System without interactions with the HPSA Portal's generic Error-Handler feature.

Figure 2-2 High-level architecture of VPN_SVP and the activation process.

Order Management

Create and manage customers

Assign service order parameters

Send service request to Service Activator

Monitor progress of service activation

Xml based request/response messages exchanged via TCP

Service Activator Portal

For non-FTA mode requests, select network resources

Select and interact with service requests that requires it

Monitor service configuration

Failure and diagnostics handling

NOTE: Throughout this guide, example values naming services and other parameters like regions and locations are used in the describtion of the operational procedures. These values are of course just examples and the actual value you must enter depends on your local configuration and procedures.

3 HPSA Inventory Management

This chapter describes HPSA inventory management and in particular the configuration of parameters and resources which are required for the successful activation of services. You may find more information on these activities in the [*ADM*].

The three standard *SAVPN* presentation trees in the Service Activator Inventory view, *Services, Equipment,* and *Parameters,* are used to display services, and to manage provider equipment and configuration parameters. These views enable you to setup Layer 2 and Layer 3 VPN service parameters as well as to generate new resources and define your supported equipment and interface types.

To illustrate VPN_SVP inventory management, we assume that the service provider intends to offer services in the "North-West" region using Cisco 3600 routers. The provider wishes to cover the region using a new sub-network which also has the name "North-West". The provider also needs to populate the inventory with additional IP addresses for the PE-CE attachment circuits. To implement this, the following tasks must be completed:

- Create new regions
- Create new locations
- Create new network and new access networks
- Create new routers
- Upload routers
- Back up routers
- Create IP address pools

NOTE: If NNM Liaison is enabled, Network Elements, Access Networks and their components may be populated into the VPN_SVP by the NNMi data load. See Chapter 4 in [*INTRO*] for more details.

NOTE: Throughout this guide, when referring to Inventory views, it as always *instance* views that is meant.

3-1 VPN_SVP Equipment Tree

VPN_SVP provides a hierarchical view of the provider networks and network elements. The (simplified) model used for the equipment hierarchy is as shown in **Figure 3-1** below.

**Figure 3-1** Simplified Equipment Model of VPN_SVP inventory
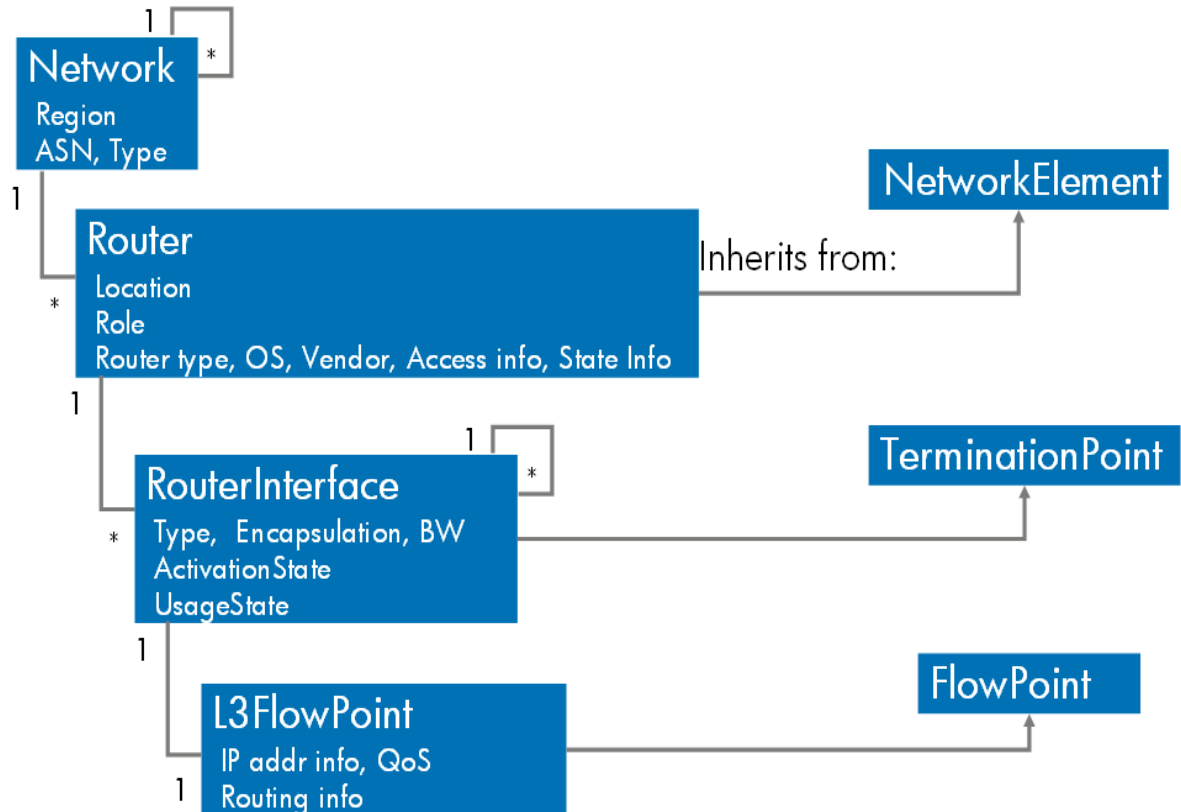
NOTE: The SAVPN/Equipment model is extended from the HPSA CRModel Equipment model. For details on CRModel Equipment model, refer to [*INTRO*]

NOTE: The terms CRModel [Common Resource Model] and CNRM [Common Network Resource Model] are used interchangeably through the documentation.

The presentation tree used to display the content of the equipment inventory (i.e. SAVPN/Equipment view) uses the Region attribute on network to further structure the view.

Follow these steps to view the SAVPN/Equipment tree view

- Log in to Service Activator.
- Select **Inventory** from the *Work Area* menu.
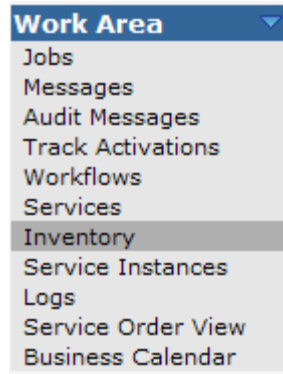
- This will open the *Inventory GUI* in a separate window.

- Once in the *Inventory GUI* window, select the **SAVPN/Equipment** instance view and then expand the *Region*→**Denmark** branch (click on the ⊞ icon).

- In region Denmark you may observe two networks: *Network Copenhagen* and *AN Copenhagen.* Expand *Network Copenhagen*→**PE routers** branch to list the existing PE routers in *Network Copenhagen*.

- Among the listed PE routers expand the router *C7600-1*→**Interfaces** to see the existing interfaces of router *C7600-1*.

You should now have a view similar to the one below in Figure 3-2 where router C7600-1 is selected for View operation.

**Figure 3-2** Inventory GUI display of Equipment hierarchy

3-2 Create New Regions and Locations

Follow these steps to create the new region "North-West".

- Log in to Service Activator.

- Select **Inventory** from the *Work Area* menu like describe in section 1-1 .

- This will open the *Inventory GUI* in a separate window.

- Once in the *Inventory GUI* window, select the **SAVPN/Parameters** view and then expand the *Parameters→SP Parameters* branch.

- To enter a new Region, right-click the **Regions** branch and select **Create Region**.
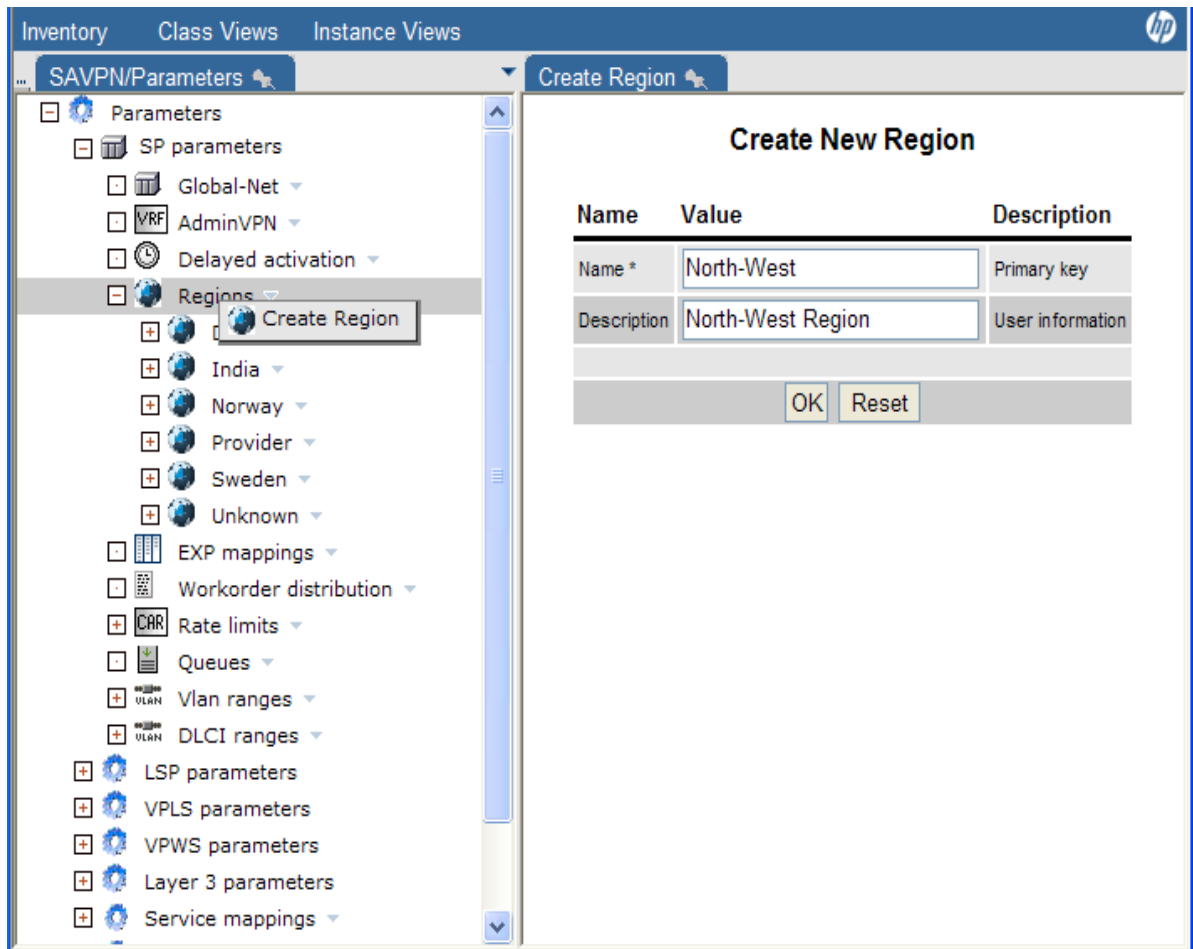
- Enter the name of the Region being added and its description.

- Select the **OK** button to submit your new region. Once the region has been created, it is possible to add Networks to it. To be able to add routers to the networks, locations must be added to the regions.

- Expand the *Regions* branch and expand the newly created **North-West** region.

- To enter a new location belonging to the region, right-click the **Locations** branch and select **Create Location.**
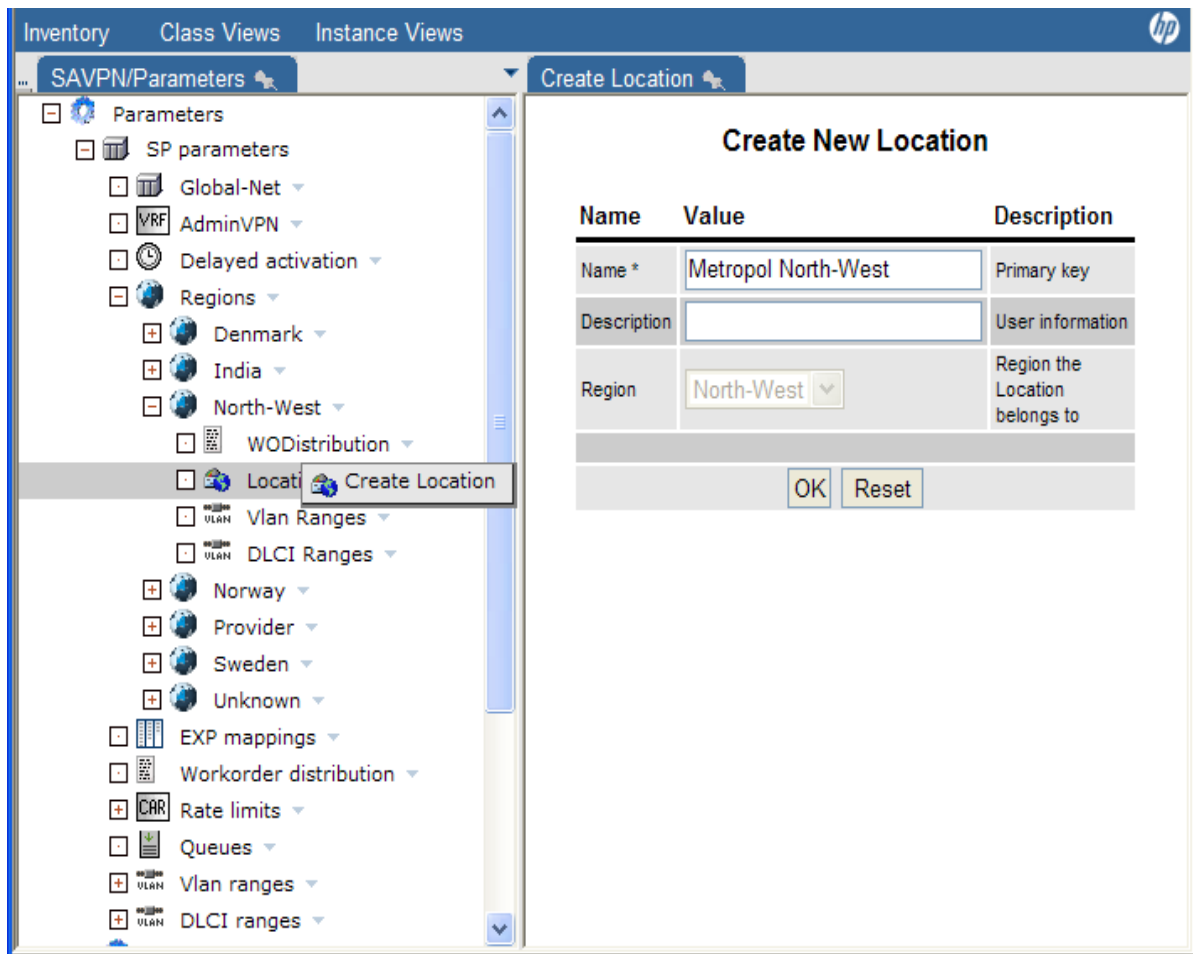
- Enter the **Name,** of the Location being added (e.g. **Metropol North-West**) and its description.
- Select the **OK** button to submit your new location.

Once the regions and location has been created, it is possible to add new routers to the networks.

NOTE: VPN_SVP associates Regions to roles so that when a service request is received, the Region of the customer's site, which is included in the request, is used to assign the access roles of the workflows executing on HPSA for that specific request.

When using Authentication on HPSA, operators (users) are assigned roles. These operator roles must match the access roles assigned to the workflows to allow the operator e.g. to view or to interact with the workflows. This means, that if an operator does not have the role corresponding to the Region specified in the request, that request will be 'invisible' to the operator.

Similarly, the *Regions* branch in the Inventory GUI's **SAVPN/Equipment** view requires that the operator has a corresponding region role assigned. Otherwise the particular region branch will not be visible.

Hence, when a new Region is created, the roles associated operators may have to be updated correspondingly. Otherwise, the new region branch will not be visible to the operator neither will the service requests for that region that might need interactions.

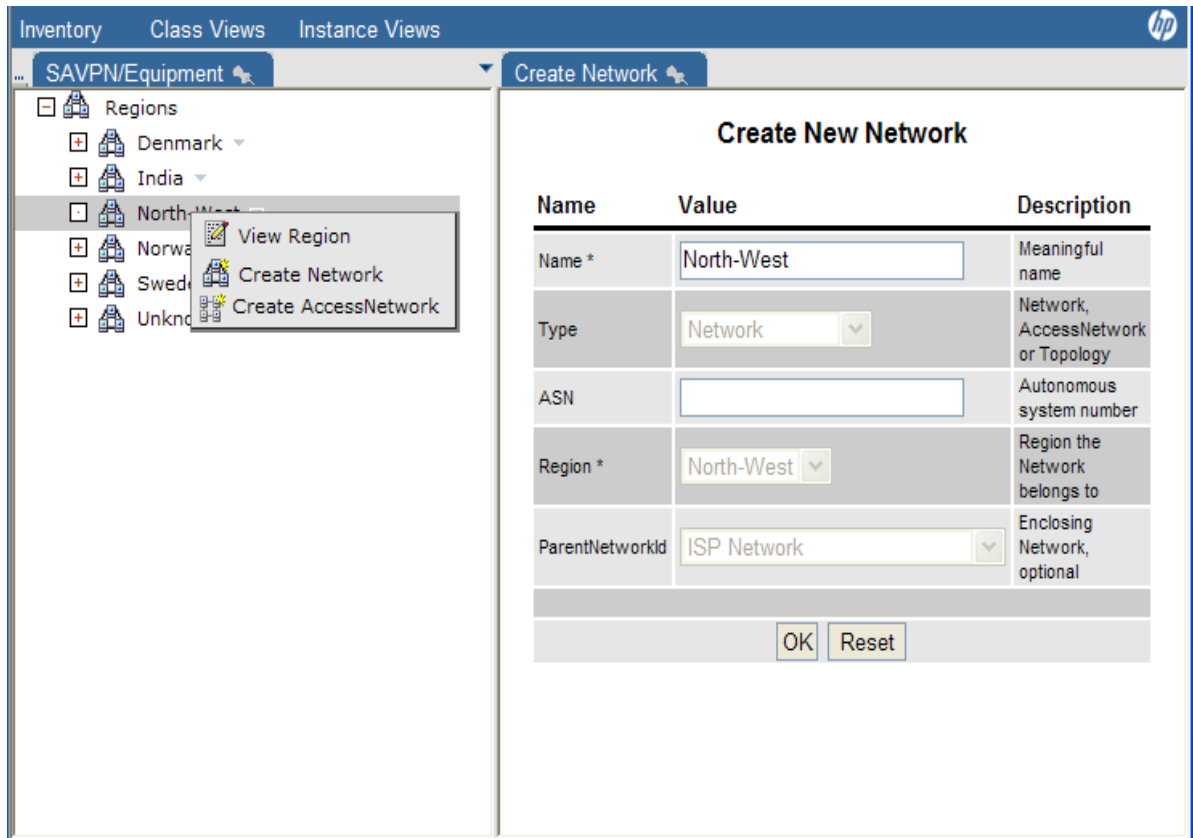You will find more information on this in the [*ADM*].

3-3 Create Vlan and DLCI Allocation Schemes

A Region and/or a Location may define a Vlan/DLCI allocation scheme specific to that Region/Location. Please see section 6-1-1 [*ADM*] for further information.

3-4 Create New Networks

Follow these steps to create the new network "North-West".

- In the *Inventory GUI* window, select the **SAVPN/Equipment** view to display the *Regions* branch.

- Expand the *Regions* branch and select the newly created region **North-West.** If you can't see the newly created region, please read the Note above!

- Right-click and select the 🏛 **Create Network** action. This will open the *Create New Network* form.

- Fill in the **Name** field.

- Note that you may optionally associate this network with an ASN (Autonomous System Number). This provides support for multi-AS-backbone scenarios. Leave it blank and the global/default ASN parameter specified in **SAVPN/Parameters** view (*Parameters→SP Parameters→<provider> ASN field*) will be used.

- Select the **OK** button to submit and create the new network. Once the network has been created, routers can be added to it.

3-5 Create New Routers

Complete these tasks to add a new Cisco 7600 router to the VPN_SVP inventory.

- In the *Inventory GUI* window, select the **SAVPN/Equipment** view to display the *Regions* branch.

- Expand the *Regions* branch and locate the "North-West" network created in above section 3-3 Create New Networks.

- Expand the network branch and right-click **PE Router**, and then select the ⚙ **Create PE routers** action. This will display the *Create PE Router* form.

- Fill in the **Name, IP Address, Passwords, Management Protocol, Vendor, OS Version** and **ElementType**.

- You may set the field PWPolicyEnabled flag, in which you can choose a password policy to apply on this Equipment from the list of PWPolicy. In such cases, you do not need to set the equipment credentials in this form.

NOTE: For more details on password policies, refer to [*INTEGRATE*].

- Remember to assign your router to the location created in section 1-1 Create New Locations. See the figure below.

- Select **BGPDiscovery** if the router type supports VPLS BGP auto-discovery (RFC 4761). This is intended for primarily Juniper type of routers. Currently Cisco routers are supported only for manual VPLS setup (RFC 4762).

- Check **Backup** field to allow backup of the newly created router. See section 3-9 Back-up and Audit of Equipment Configuration below.

- Select the **OK** button to create a new router. The router will be stored in the HPSA inventory.

NOTE: When a new router is added to the inventory, its **LifeCycleState** is set to *Planned*. In practice, the service provider's network engineers would later install the newly added PE router and provide it with its initial configuration.

When the new router has been installed in the network and its initial configuration has been applied including its IP addresses, its **LifeCycleState** must manually be set to *Accessible* indicating that it is possible to connect from VPN_SVP to the router.

When the **LifeCycleState** is set to *Accessible*, the Interface Upload tool may be used to upload and create the interfaces and controllers of the router in Inventory. See section 3-6 below.

It is possible for the network engineer to configure the description fields on (some of) the interfaces in the router's configuration. E.g. interfaces to be used for other purposes but VPN services may be marked with the key word RESERVED. Interfaces may also be marked with the key word UPLINK. In both cases, these interfaces when upload into the Inventory, will be put in Reserved state and not be selectable for VPN service attachments. When this pre-configuration has been completed, the **LifeCycleState** must manually be set to *Preconfigured*.

When in **LifeCycleState** *Preconfigured*, and the interfaces have been uploaded, the **LifeCycleState** will automatically be set to *Ready* indicating that the router is ready for service activation.

It is possible to use the Interface Upload tool also when the **LifeCycleState** is *Ready* e.g. the router has been updated with more interface cards.

Inventory   Class Views   Instance Views

SAVPN/Equipment   ▼ | Create PE routers

☐ 🏠 Regions
  ⊞ 🏠 Denmark ▾
  ⊞ 🏠 India ▾
  ☐ 🏠 North-West ▾
    ☐ 🏠 North-West ▾
      ☐ 🖧 PE routers ▽
      ☐ 🖧 | 🖧 Create PE routers
      ☐ 🖧 ASBR routers
  ⊞ 🏠 Norway ▾
  ⊞ 🏠 Sweden ▾
  ⊞ 🏠 Unknown ▾

Create New PERouter

Name	Value	Description
NetworkId	106	Network the NE belongs to
Name *	Juniper-3	Meaningful name of the device
Description	PE Router	User information
Region	North-West	Region the Network belongs to
Location *	Metropol North-West ⌄	Location of the device
Loopback IP	172.16.0.2	Primary IP address of the device
Management IP	193.88.72.102	IP address for management of the device
Management Protocol	telnet ⌄	
PWPolicyEnabled	☑	True if this NE use a password policy to authenticate
PWPolicy	PE_Password_Policy ⌄	Name of the password policy
UsernameEnabled	☐	True if username is used to authenticate management connection
Password		Password for management connection
EnablePassword		Password to enable device configuration
Vendor	Juniper ⌄	Vendor of device
OSVersion	Juniper-9.4R2.9 ⌄	OS version of device
ElementType	M7i ⌄	Type of device
BGPDiscovery	☐	NE supports VPLS BGP discovery (rfc 4761)
Tier	2	Tier levels for routers
NextTier	Juniper-1 ⌄	Reference to the downstream neighbor tier PE router
NextTier2	J2300-1 ⌄	Reference to a optionally second downstream neighbor Tier1 PE router for a dual homed Tier2 router
SerialNumber	123-456-789	Serial number of the device (inventory information)
Role	PE	Role of device in the network
AdminState	Up ⌄	Up, Down, Unknown, Reserved
LifeCycleState	Ready ⌄	Planned, Preconfigured, Accessible, Ready
Backup	☐	Backup tool enabled for the router
SchedulingPolicy	-none-	PE backup scheduling policy
ROCommunity	ro	SNMP read-only community string
RWCommunity	rw	SNMP read-write community String
NNMI UUId		Universal identifier of corresponding NNM object
NNMI Id		Identifier of corresponding NNM object
NNMi Last Update		Time the object was last updated/refreshed from NNMi. Format: [dd-MM-yyyy]. Example: [30-11-2010]

OK   Reset

NOTE: Two new attributes, NextTier and NextTier2 are included to extend the LSP functionality. The tiers define a hierarchy among the PE routers with Tier1 being the PE router closest to the MPLS core and the higher Tiers being successively farther from the MPLS core. A current maximum hierarchy of 3 tier levels is supported.

The attribute NextTier is mandatory for a Tier2/3 router, ignored for a Tier1 router

The attribute NextTier2 is optional for a Tier2 router, ignored for other tier routers.

When adding a PE router, the form accepts entering a Tier value. If the value "1" is entered, nothing further happens and the form may be submitted.

If "2" is entered, one or optionally two downstream Tier1 routers must be appointed as NextTier and NextTier2 from a selection list populated with the available Tier1 routers.

If "3" is entered, one downstream Tier2 router must be appointed as NextTier from a selection list populated with the available Tier2 routers.

The selection list will contain Tier routers in the same Region as the PE router.

3-6 Upload Interfaces of Router

Follow these steps to upload your router.

- In the *Inventory GUI* window select the *SAVPN/Equipment* view.

- Expand the *North-West* region branch and locate the "North-West" network created in 3-3 Create New Networks.

- Expand the network branch and locate the router **C3600-2** created in 3-5 Create New Routers above.

- Right-click and select the 🖧 **Upload Router** action (LifeCycleState must be changed to e.g *Preconfigured* for Upload action to appear - See Note above). This will open the Upload Interfaces form.

- In the form you may specify a slot number to upload only the interfaces and controllers associated this slot, or you may leave the field blank to upload all interfaces and controllers.
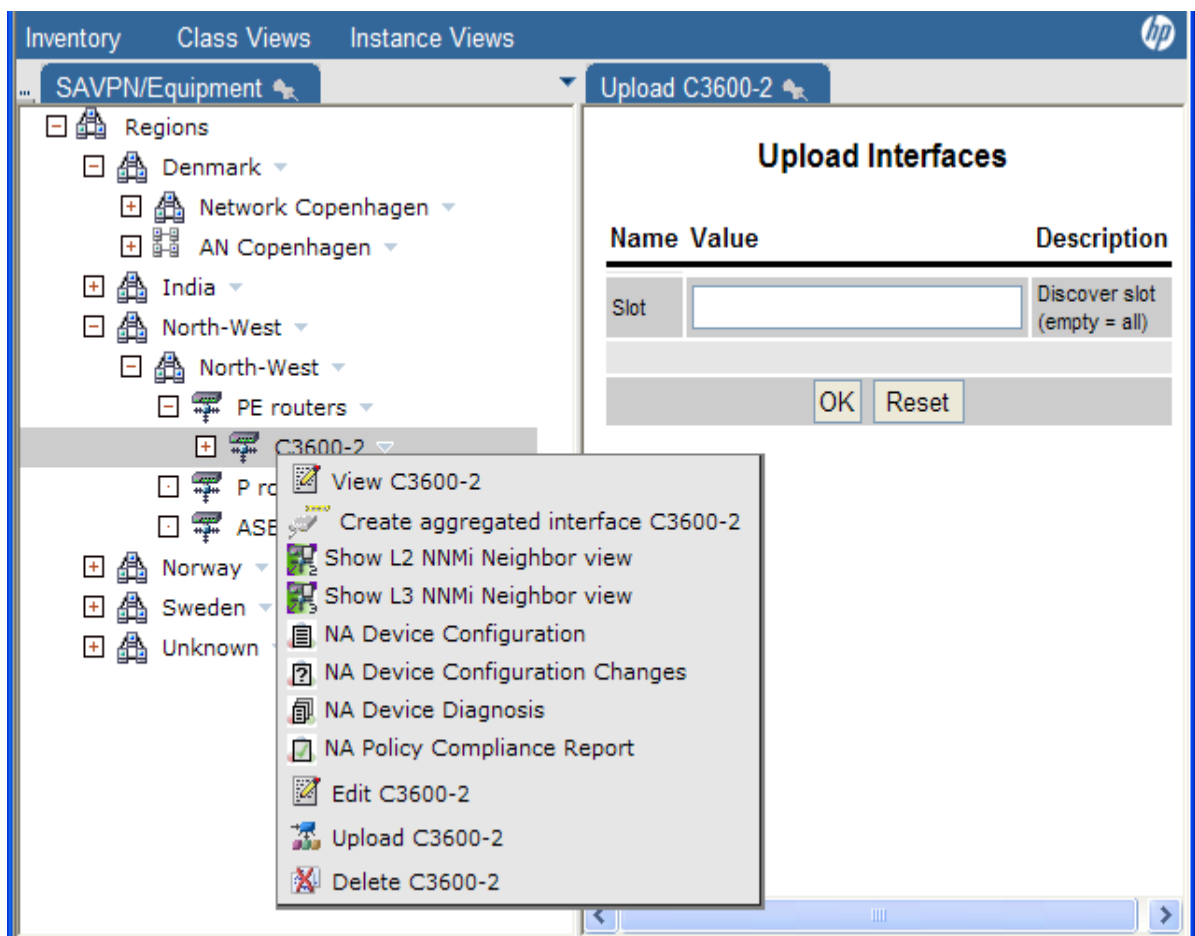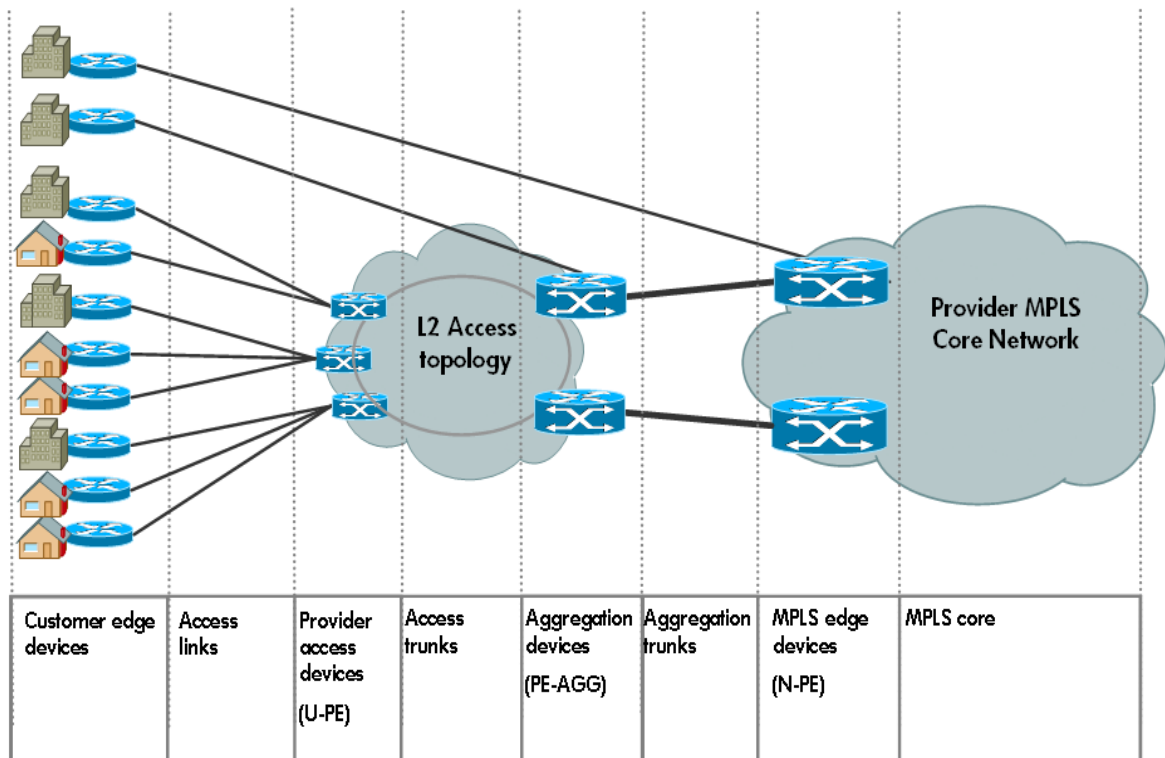

- Now select the **OK** button to upload your router.

- HPSA will then connect to the router, perform an upload of the configuration, parse this for the interface information and populate the inventory with the discovered interfaces and E1/STM1 controllers.

NOTE: When you right click on the router, you will also see several NA and NNM related actions. For details on the events that occur on choosing these options, refer to Chapters 11 and 12.

3-7 Create New Access Networks

VPN_SVP supports creation and configuration of L2 Ethernet switch based access networks. Access networks provide connectivity of customer services entering via access links on the provider's access device ports to the MPLS edge devices. See schematic architecture in **Figure 3-3** below.

Figure 3-3 Access network Architecture

Customer edge devices	Access links	Provider access devices (U-PE)	Access trunks	Aggregation devices (PE-AGG)	Aggregation trunks	MPLS edge devices (N-PE)	MPLS core

The access network is connected to the provider's MPLS edge device (PEs or N-PEs) via L2 aggregation trunks. These trunks carry each service on a specific Vlan id. The Vlan id is assigned by the provider at the access port as either customer specific or provider selected.

The access network may consist of multiple access topologies each which may be rings or linear topologies of access devices (U-PEs) being attached to one or more aggregation device.

The assigned Vlan id is added to the access port, to the trunks of the access topology that contains the access devices (U-PE) and aggregation devices and to the aggregation trunks connecting to the PE devices as an integral part of the VPN_SVP activation process.

The access network component is agnostic about the nature of the service being attached and provides the basic connectivity from access port to MPLS edge N-PE device. Services may be attached to access devices, aggregation devices and of course also as direct attachment onto PE devices.

3-7-1 Adding New Access Network

You may use the Inventory GUI to perform this task. In large deployment scenarios, it may be more efficient to generate the information to load in proper formatted XML files and use the XML Importer tool to accomplish this task.
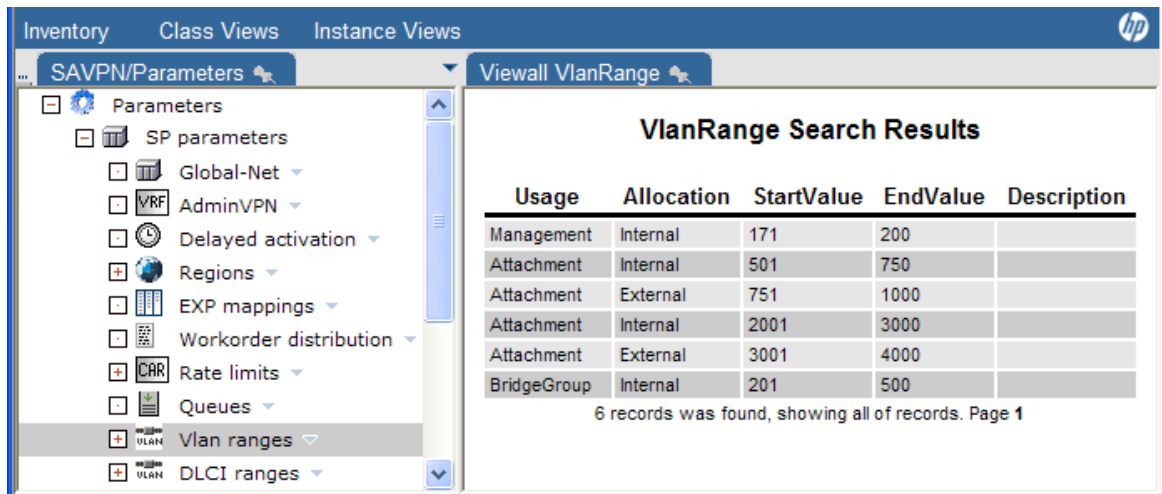
Follow these steps to create the new access network "*AN Copenhagen*" in region *Denmark*.

- In the *Inventory GUI* window, select the **SAVPN/Equipment** view to display the *Regions* branch.

- Expand the *Regions* branch and select the region **Denmark**.

- Right-click and select the ⬛ **Create AccessNetwork** action. This will open the *Create New Network* form.

- Fill in the **Name** field. E.g. "*AN Copenhagen*"

- The **ManagementVlans** field allows you to reserve a range or list of Vlan ids used for management access to the NEs of the access network. These values will not be used for services. The list of management Vlan ids must be taken from the range defined in the **Vlan ranges** defined in Inventory GUI's *SAVPN/Parameters→Parameters→SP parameters* branch.

NOTE: The global allocation scheme of Vlan ids may be configured using Inventory GUI's **SAVPN/Parameters→Parameters→SP parameters→Vlan ranges** object.

The range *'Attachment/Internal'* represents provider selected values being allocated by VPN_SVP for access network use and the range *'Attachment/External* represents the range from which user selected values will be allocated.

The scheme may be configured to suit your specific purposes and will be followed by VPN_SVP allocation Vlan ids for different services.

The scheme (illustrated above) may be global in the sense, that the same scheme will be followed on all access networks and PE routers, but values will only be unique within each access network and its attached N-PEs. Hence, the same Vlan id may be used in different access networks (attached to different N-PEs).

Vlan schemes may be specific to a Region and/or a Location by defining a Vlan ranges object per Region/Location.

If a Location specific range is defined that will be used for requests in that Location. If not, but the containing Region specifies a range that will be used. Otherwise the global specified range will be used.

- Select the **OK** button to submit and create the new network. Once the network has been created, aggregation devices can be added to it.
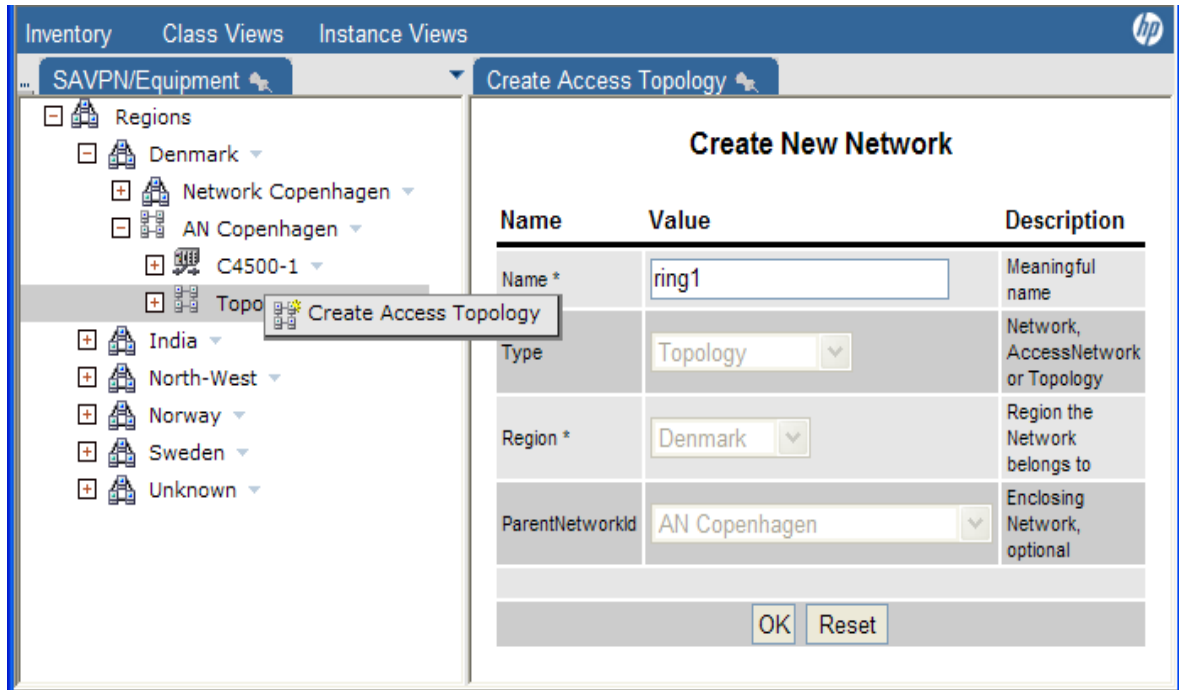
Follow these steps to create a new aggregation device for the newly created access network "*AN Copenhagen*":

- In the *Inventory GUI* window, select the **SAVPN/Equipment** view to display the *Regions* branch.
- Expand the *Regions* branch and locate the "*AN Copenhagen*" access network created above.
- Right-click and select the 🖳 **Create Aggregation switch** action. This will open the *Create Aggregation switch* form.
- Fill in the form as described in section 3-5 above to create e.g. a Cisco4500 aggregation switch.
- Follow the steps described in section 3-6 to upload the interface information of the switch.

When an Aggregation switch has been created and its interfaces uploaded/initialized, you may add topologies to the aggregation switch.

Follow these steps to create a new access topology in to the newly created access network "*AN Copenhagen*":

- In the *Inventory GUI* window, select the **SAVPN/Equipment** view to display the *Regions* branch.

- Expand the *Regions* branch and locate the "*AN Copenhagen*" access network created above.

- Expand the access network branch "*AN Copenhagen*".

- Right-click the **Topologies** branch and select the 🔲 **Create Access Topology** action. This will open the *Create Access Topology* form.

- Fill in the **Name** field to create e.g. access topology *ring1.*

- Select the **OK** button to submit and create the new topology (sub-network). Once the topology has been created, access devices can be added to it.

Follow these steps to create new access devices for the newly created topology (sub-network) "*ring1*":

- Expand the *Topology* branch and locate the "*ring1*" topology (sub-network) created above.

- Right-click and select the 🔲 **Create Access Switch** action. This will open the *Create Access Switch* form.

- Fill in the form as described in section 3-5 above to create e.g. a Cisco3400 access switch, "*C3400-1".*

- Follow the steps described in section 3-6 to upload the interface information of the newly added access switch.

When an access switch in a topology has been created and its interfaces uploaded/initialized, you may **attach** the topology to the aggregation switch.

Follow these steps to **attach** the newly created topology "*ring1*" to the aggregation switch:

- Expand the access network branch "*AN Copenhagen*" and locate the "*C4500-1*" branch corresponding to the aggregation switch created above.

- Right-click the **C4500-1** branch and select the ⚙ **Attach Access Topology** action. This will open the *Create Link* form.

- You must now select from the TermionationPoint1 drop-down list, the port on the aggregation switch C4500-1 to be used as the interconnecting trunk port. E.g. *GigabitEthernet1/1*.
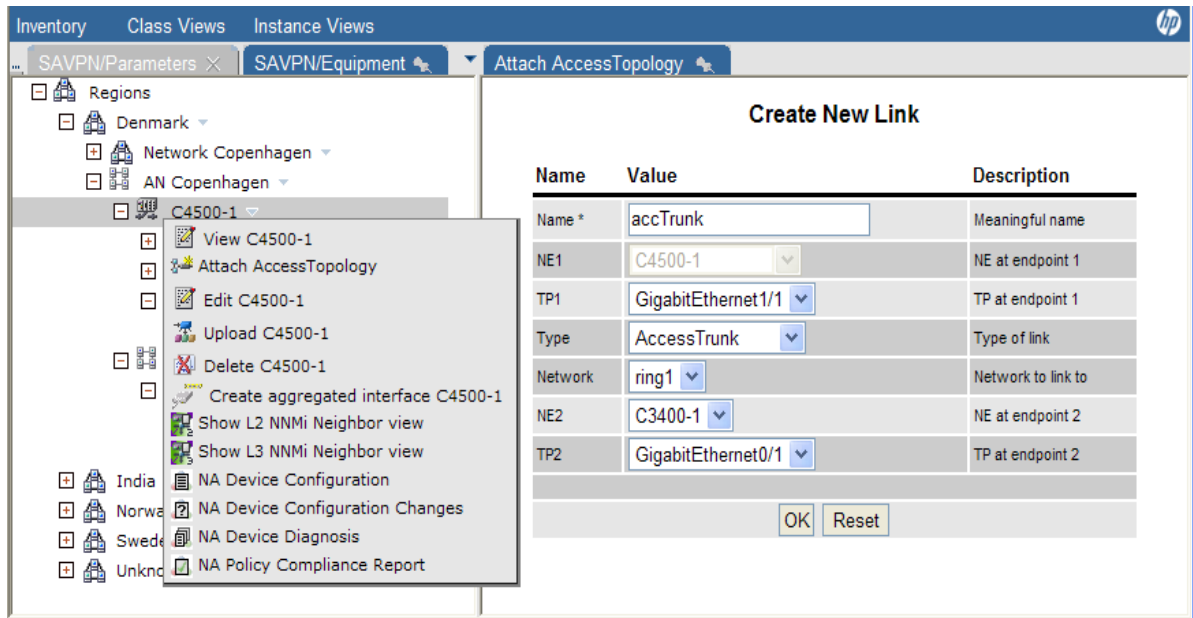
- Select from **Type** drop-down list, AccessTrunk, so that Aggregation Switch can be connected to the Access Switch

- Select from **Network** drop-down list, ring1.

- Select from the **TermionationPoint2** drop-down list, the port on the access switch *C3400-1* to be used as the trunk port, e.g. *GigabitEthernet0/1*.

- Select the **OK** button to submit and attach the new topology (sub-network) ring1 to the aggregation switch C4500-1. This creates a trunk object representing the link between the *C3400-1* access switch and the *C4500-1* aggregation switch.

The process describe above may be used to e.g. create a second aggregation switch, e.g. C4500-2 to which the topology *ring1* also may be attached (to form a ring). Likewise multiple access switches per topology and multiple topologies may beF added and attached to the aggregation switches.

The individual trunk ports used for the links between access switches of the same topology and used to interconnect the two aggregation switches must also be created in Inventory.

Follow these steps to create a **trunk** between the two aggregation switches:

- Expand the access network branch "*AN Copenhagen*" and locate and expand the aggregation switch branch "*C4500-1*" corresponding to one of the aggregation switches created above.

Right-click the **Trunks** branch and select the ⚙ **Create Link** action to create Aggregation Trunk. This will open the *Create Link* form.
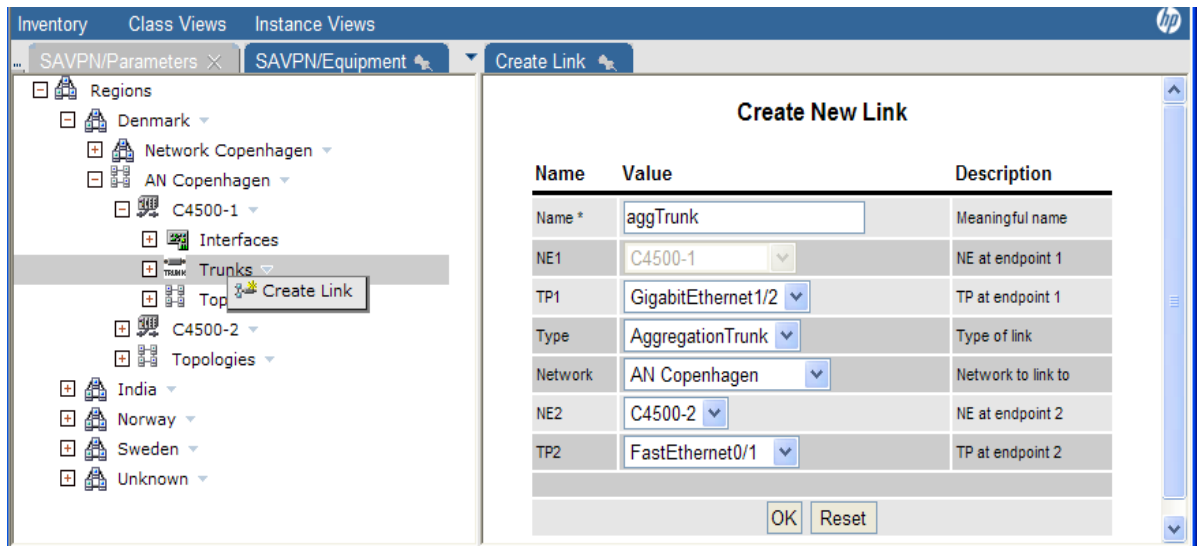
- You may select the port on the aggregation switch "*C4500-1*" to be used to link to the other aggregation switch from the **TP1** drop-down list, e.g. GigabitEthernet1/2.

- Select from **Type** drop-down value AggregationTrunk.

- Select from the **Network** drop-down value AN Copenhagen.

- You may select the other aggregation switch you created above (e.g. "*C4500-2*") from the **NE2** drop-down list and the port on this to be use for the link, e.g. *FastEthernet0/1*.

- Select the **OK** button to submit and create the new trunk link between aggregation switches *C4500-1* and *C4500-2*.

- You should follow similar steps in creating the trunks between your access switches.

You have now created a simple access network similar to the Inventory view illustrated below. Note the Trunk(100) information on the two aggregation switches represent the link between these.

You are not quite complete with the process yet. You must now proceed and attach the created access network to the MPLS edge devices in you network (N-PEs) as described in section 3-7-2 below.

NOTE: The process described in this section updates the Inventory db to match your access network configuration. There are no activation activities (device configurations) in the above process. When services are activated, this inventory information allows VPN_SVP to configure the relevant trunks ports with allocated Vlan ids to provide the connectivity of user date from the access port to the N-PE termination point.

3-7-2 Attaching Access Network to MPLS Edge

The final step in creating your access network is to attach it to the MPLS edge devices, refer to the architecture illustrated in **Figure 3-3** above.

You must decide on witch N-PE router to attach to the access network and select this in the Inventory GUI. Follow these steps to select your N-PE router:

● In the *Inventory GUI* window, select the **SAVPN/Equipment** view to display the *Regions* branch.

● Expand the *Regions* branch and select the region **Denmark** corresponding to the region in which you created the access network as described in section 3-7-1 above.

● Locate and expand the network branch "*Network Copenhagen*" which represents you MPLS devices.

● Expand the **PE router** branch and right-click the desired N-PE device, e.g. *C7600-1*.

● Select the **Create Link** action to create Aggregation Trunk. This will open the *Create Link* form.
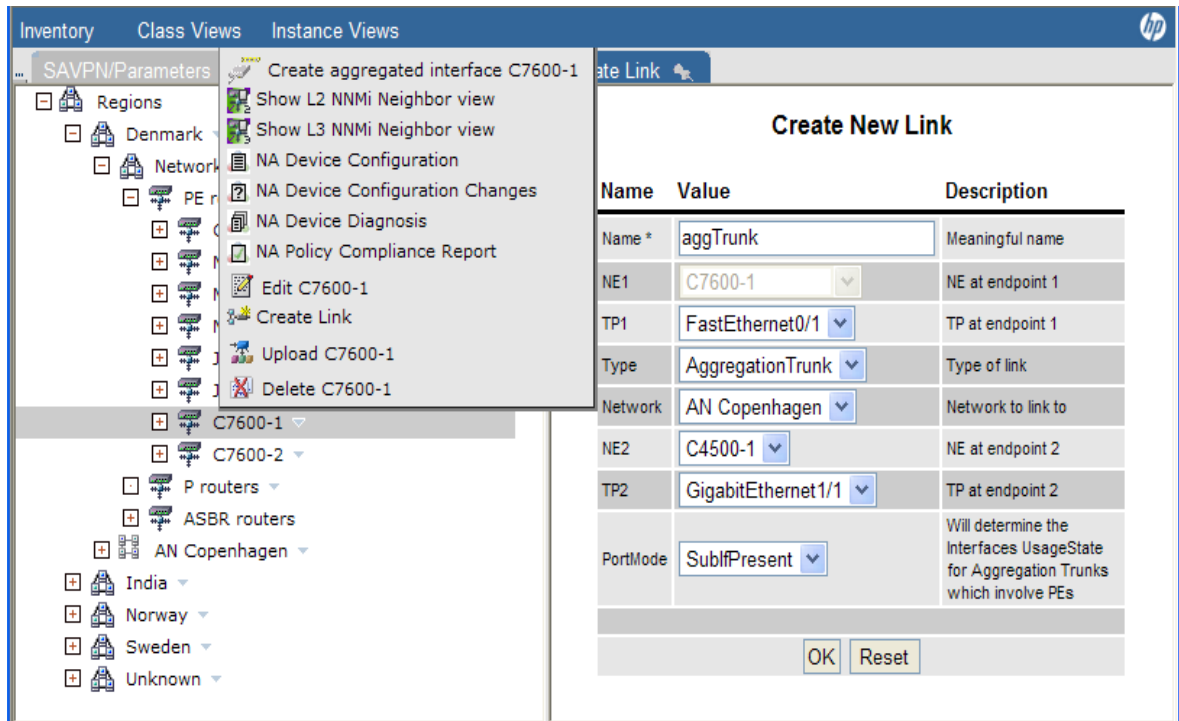
- Select the **TerminationPoint1** on your selected N-PE from the drop-down list of ports, e.g. *FastEthernet0/1*.

- Select the **Type** from drop-down list as Aggregation Trunk.

- Select the **Network** from the drop down list, e.g. *AN Copenhagen*. Select the **AggregationSwicth** from the drop down list, e.g. *C4500-1.* Select the **TerminationPoint2** on your selected aggregation switch from the drop-down list of ports, e.g. *GigabitEthernet1/1*.

- Select the N-PE PortMode. Mode SubInterface or Switchport is supported. Currently Cisco devices require SubInterface mode to support L2 VPWS service and SwitchPort mode to support L2 VPLS service. Hence, to support all service types at least two attachment ports must be defined, one of each type.

- Select the **OK** button to submit and create the new trunk link between the N-PE *C7600-1* and the aggregation switches *C4500-1*.

- Follow the same procedure to attach the access network to a redundant N-PE, e.g. *C7600-2* using aggregation switch *C4500-2*.

The access network architecture you have now completed is similar to the one illustrated in **Figure 3-3** above.

You may now use the access ports on the access switches in your topologies to attach customer services. For more information on how to do that, see section 7-2 .

NOTE: The process described in this section updates the Inventory db to match your access network configuration. There are no activation activities (device configurations) in the above process. When services are activated, this inventory information allows VPN_SVP to configure the relevant trunks ports with allocated Vlan ids to provide the connectivity of user date from the access port to the N-PE termination point.

CAUTION: When services have been provisioned via access networks, a set of allowed Vlan Ids will have been added to the trunk ports.

Now, adding or removing an access network device (switch) is possible and the connectivity may be re-configured via the Inventory GUI as described above, but the new trunk ports will not be configured with the existing set of allowed Vlan Ids!

You must make this allowed Vlan configuration on the switch itself and then use the Upload Interface facility (see section 3-6) to make the inventory data synchronized with the network device (switch) configuration.

3-8 Multi-AS-Backbone Networks

Layer 3 VPN services are supported across a provider core network consisting of Multi-AS Backbones, i.e. multiple Autonomous Systems (ASs) interconnected with links between AS Border Routers (ASBRs). When a site is selected like e.g. Site 4 in the **Figure 3-4** below for a L3 service, the ASBR links will also be activated with a service specific Vlan interconnecting the ASs in a VRF back-to-back mode.

Figure 3-4 Multi-AS-backbone network topology
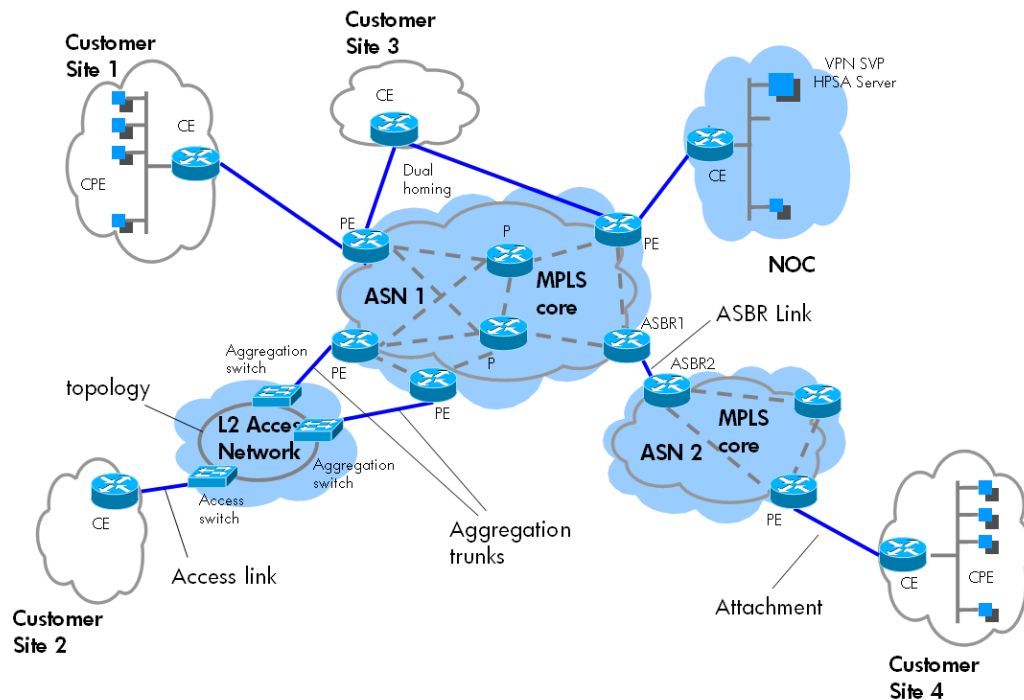
3-8-1 Create ASBR Link

Let us assume a use case with ASN1 in Network Copenhagen belonging to region Denmark and ASN2 in Network Stockholm in the region Sweden.

Let us further assume that ASN1 has a value of 12345 and ASN2 has a value of 10101.

First step towards creation of an ASBR link is to appoint the ASBR routers on either Networks that have the physical connection to each other.

- In the *Inventory GUI* window, select the **SAVPN/Equipment** view to display the *Regions* branch.

- Expand the *Regions* branch, expand the region **Denmark** and expand the *Network Copenhagen* branch.

- In **Network Copenhagen**, expand the *PE routers* branch. ASBR routers are assumed to have role PE routers.

- Right click on the PE router that will also be acting as an ASBR router, and select the option ![icon] **Create Link**.
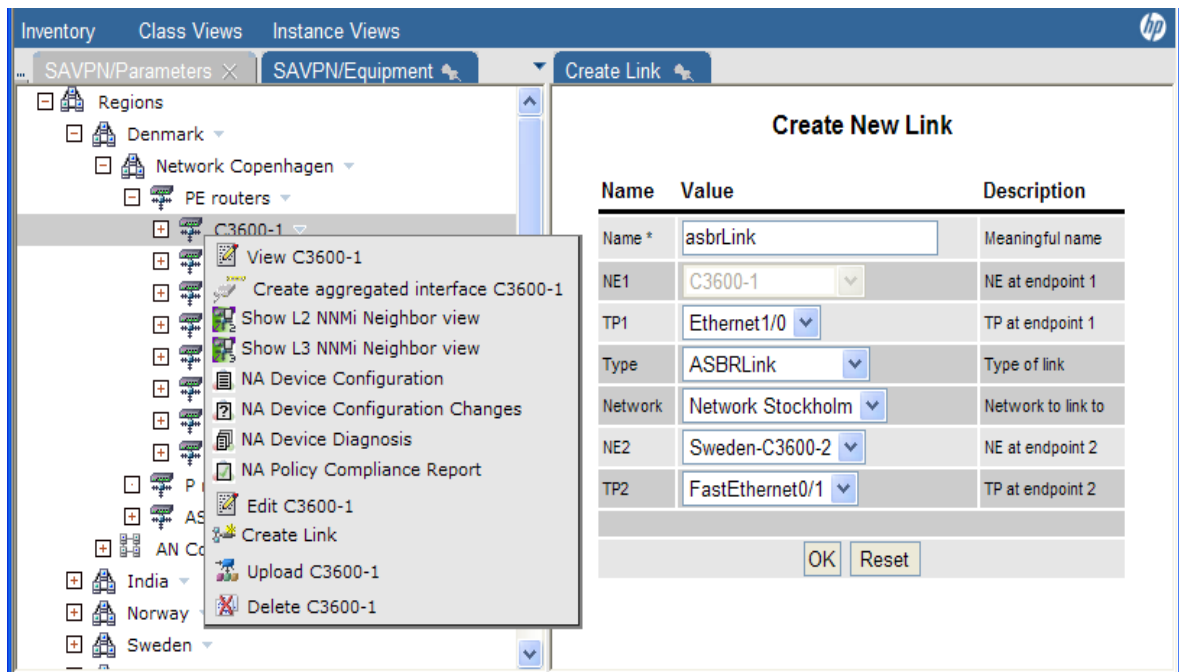
- Choose in this AS (12345), the Termination Point (TP1) that would be dedicated as a ASBR port on the selected NE (NE1)

- Select **Type** as ASBRLink

- Choose for the remote AS (10101), the network (Network2), the remote NE (NE2) and the termination point (TP2) on the remote NE. Note by selecting the network, the remote ASN is displayed.

- Click on OK to create the ASBR Link between Network Copenhagen and Network Stockholm.

NOTE: The ASN values can be set at the Network level, in which case, all the equipments created under this network uses the Network level ASN. In case no ASN value is defined at the network level, the equipments in this network use the ASN defined at the SP level, which is the default ASN.

You have now created in the Inventory, the logical object (ASBRLink) that represents the physical connectivity between the ASs. The actual physical connectivity has to be established in the network manually.

At service provisioning time, the inventory ASBRLinks will be used to identify the connectivity available between the ASs and to select on which the virtual links will be created to carry the service specific data.

You may view and inspect the created ASBR Links by following these steps:

- In **Network Copenhagen**, expand the *ASBR routers* branch.

- Right click on the ASBR router on which you want to inspect the ASBRLinks and expand the *ASBRLinks* branch.

- Select a ASBRLink from the list and view the details in the right pane as shown in the figure below.
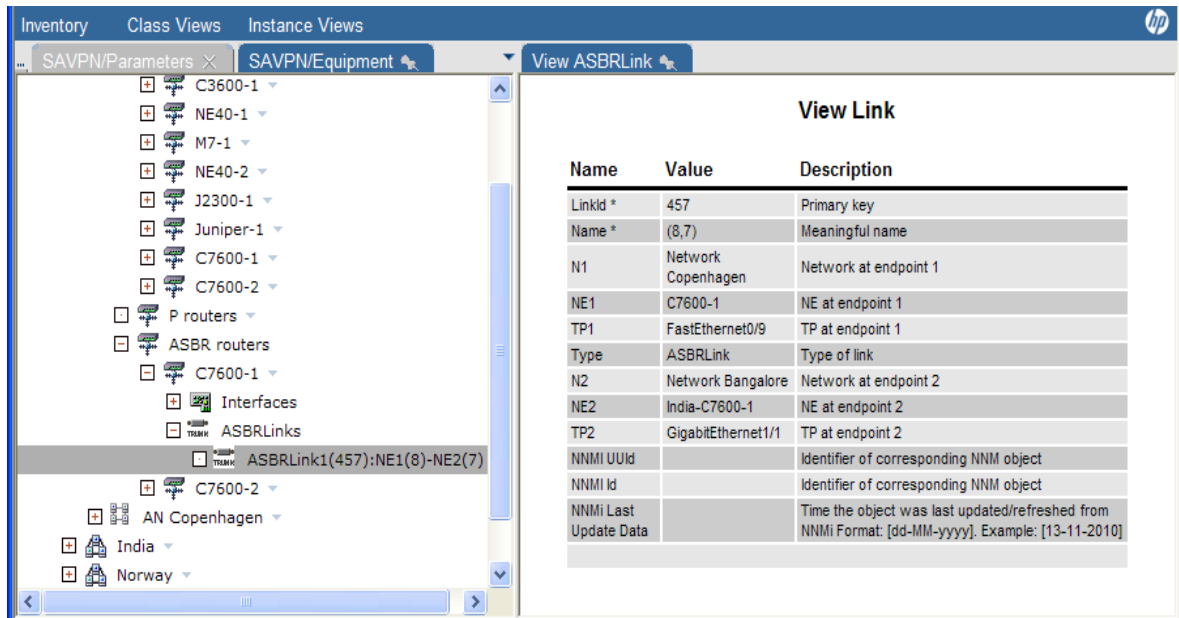
3-9 Back-up and Audit of Equipment Configuration

Router configuration management is performed through the *Tools→Backup* menu.

The Backup tool allows the service provider to back- up the configuration files of the routers into the HPSA inventory database. The tool allows backup of both the *running-config* and the *startup-config*. Multiple versions of configuration files for each router may be stored in the HPSA inventory.
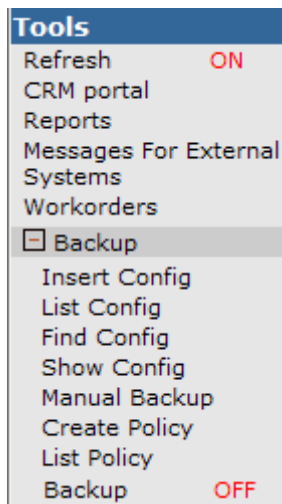
Before the backup operation can be performed, set the value for the field **BackupDirectory** under **SAVPN/Parameters→Parameters→SP parameters→Global-Net.** This is the location where the equipment configurations are stored by the backup tool.

Also provide the value for the field **IP** under **SAVPN/Parameters→Parameters→SP parameters→Global-Net.** This is the IP address of the VPN SVP server, used by e.g. TFTP.

Follow these steps to backup your router.

- Select **Backup** from the *Tools* menu.

- Select **Manual Backup** from the **Backup** menu. This will open the *Back-up Equipment Configuration* form
- Select in the Equipment name selection list the router created above, C3600-2

NOTE: In the *Equipment Name* list, only the routers in Inventory Equipment tree which have the *Backup* attribute set to *Yes* are selectable. See section 3-5 Create New Routers.

Back-up Equipment Configuration

Back-up an Equipment Configuration	
Equipment Name:	C3600-2
Target Memory:	startup-config

Create Backup

- Select the configuration memory type of the router. For Cisco devices, this will typically be *startup-config* or *running-config*.

NOTE: In the **Target Memory** list, the vendor specific types of configuration files are listed. For Cisco these includes *startup-config* and *running-config*, for Juniper only *active* type is supported.

When adding ElementTypes in Inventory- Parameters tree, the generic **TargetType** *startup* or *running* may be associated the vendor specific memory types.

- Press **Create Backup** to fetch the startup configuration of the C3600-2 router
- HPSA will then connect to the router, perform an upload of the startup-config using the TFTP protocol and populate the database with the configuration file.

Stored configuration files can be viewed, manually edited and restored onto the router. The configuration files may also be cloned to create copies that may be restored to other routers

- To view a stored configuration file, select **List Configs** in the left navigation pane in the **Backup** menu. This will open the *Router Configuration* view
- Expand one of the entries to see the existing backups

Routers

Cisco | **Juniper**

Router Name						
⊟	India-C7600-2					
⊟	C3600-1					
	Time Stamp	Version	Retrieval Type	Memory Type	Created By	Comment
	2010.11.30 20:08:44	1.0	MANUAL	startup-config	admin	
⊟	C7600-2					
⊟	Sweden-C3600-1					
⊟	C7600-1					
⊟	India-C7600-1					
⊟	Sweden-C3600-2					
⊟	C4500-1					
⊟	C3400-2					
⊟	Norway-C7600-1					
⊞	C3400-1					

- Right-click on the desired backup entry and select **View**. This will display the *View Equipment Configuration* form

View Equipment Configuration

Update Equipment Configuration	
Equipment Name	C3600-2
Timestamp	2008.05.28 11:58:38
Version	1.0
Retrieval Type	manual
Memory Type	startup-config
Created by	admin
Modified by	
Comment	

Data

```
!
! Last configuration change at 13:29:57 UTC Wed May 25 2005
! NVRAM config last updated at 13:29:58 UTC Wed May 25 2005
!
version 12.2
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
no service password-encryption
service compress-config
!
hostname cisco
!
logging count
aaa new-model
!
```

The Backup Audit tools allow the provider to compare or Audit a configuration file stored in the HPSA inventory with the current configuration file on the router. Lines which have been inserted, modified or deleted will be marked with different colors.

- To perform a configuration audit, select **List Configs** in the left navigation pane in the *Backup* menu. This will open the *Router Configuration* view

- Expand one of the entries to see the existing backups

- Right-click on the desired backup entry and select **Audit**. You may now select the **Target Memory** you want to audit your stored db version against.

- Press the **Audit** button to generate the view.

The Backup tool provides configuration of backup polices that allows automated scheduled periodic backups of routers.

- To perform scheduled backup, turn the Backup *ON* in the left pane. Additional scheduling policies may be created by selecting **Create Policy** in the left pane.

- List of existing backup policies can be viewed by clicking on List Policy in the left pane. The Default backup policy can not be deleted. It can only be modified. The operator created backup policies can be modified or deleted by right clicking on the policy.

Policies found (2)			
Name	Starting Time	Periodicity	Backup Number
Default	2010.11.29 14:40	Daily	5
dailyBackupPolicy	2010.11.30 00:00	Daily	1

- After creating a Backup policy, a router may be associated the new backup scheduling policy. Edit the router in the Inventory Equipment tree and select the new policy in the **SchedulingPolicy** selection list. See section 3-5 Create New Routers.

3-10 Create IP Addresses

The VPN_SVP administers the IPv4 and IPv6 addresses used for the Layer 3 attachment circuits between PE and CE router and optionally the loop-back IP addresses allocated to managed CE routers. Additionally, VPN_SVP administers IPv4 addresses for Multicast services, LSP endpoints and more, see below. These addresses are stored in the HPSA inventory as resources and will be marked as reserved when in use.

The Service Provider operator is required to pre-populate the HPSA inventory IP address pools with addresses through the inventory view.

Follow these steps to create an IPv4 address pool for PE-CE attachment circuits.

- Navigate to the *Inventory GUI* window.
- Select the *Parameters* view and expand the *Parameters* branch.
- Navigate to and expand the *Layer 3 parameters* branch.
- Right-click the *Address pools* branch and select **Create AddressPool** action. This will open the *Create New IPAddrPool* form.
- Fill e.g. **Name** as PE-CEUnique, **IPNet** as 192.0.0.0 and **Mask** as 16. This defines the pool PE-CEUnique to contain addresses in range of 192.0.0.0/16.
- Select **Type** IPNet for PE-CE attachment circuit addresses.
- Select AddressFamily as IPv4 and submit (press OK). Similarly, select AddressFamily IPv6 and the relevant IPv6 IPNet/mask to create an IPv6 address pool.

- Now, to populate the pool with IP net entries, expand the *Address pools* branch
- Right-click PE-CEUnique and select the **Create Address** action. This will open the *Create Address* form.
- IP net entries can be generated by e.g. providing these values: **First IP network**: 192.0.2.0/30 (the ip network address and mask of the next entry to be populated), **Number**: 20 (the number of new IPNet entries to generate)
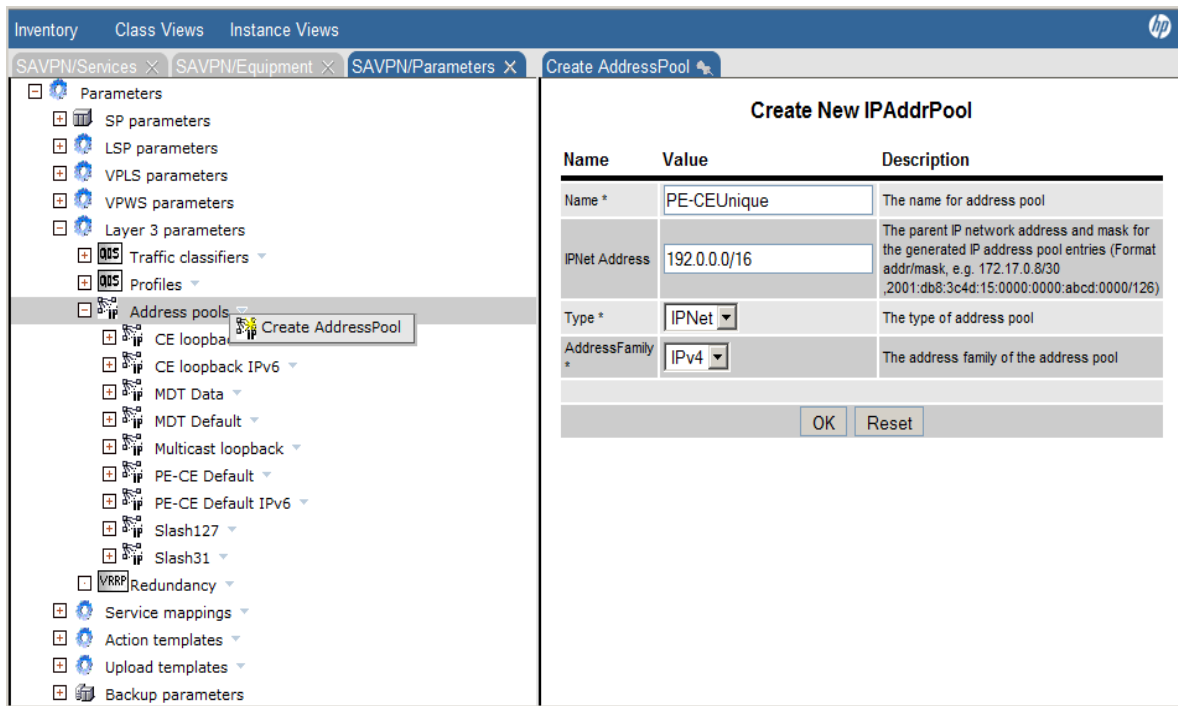
Different types of IPv4 address pools are supported. Besides attachment circuit addresses and CE loopback addresses, these include LSP loopback addresses and the following multicast related pools:

- MDT Data
- MDT Default
- Multicast loopback

See [*ADM*] for further information on creating the different types of IP address pools.

3-11 Manage Activation Parameters

The provider controls most of the technical activation parameters through the *SAVPN/Parameters* view in the *Inventory Tree*.

These parameters include default Autonomous System Number (ASN), Admin VPN, Regions and Locations, Traffic Classifiers and QoS Profiles, Router models etc. See the [*ADM*] for further information on these parameters.
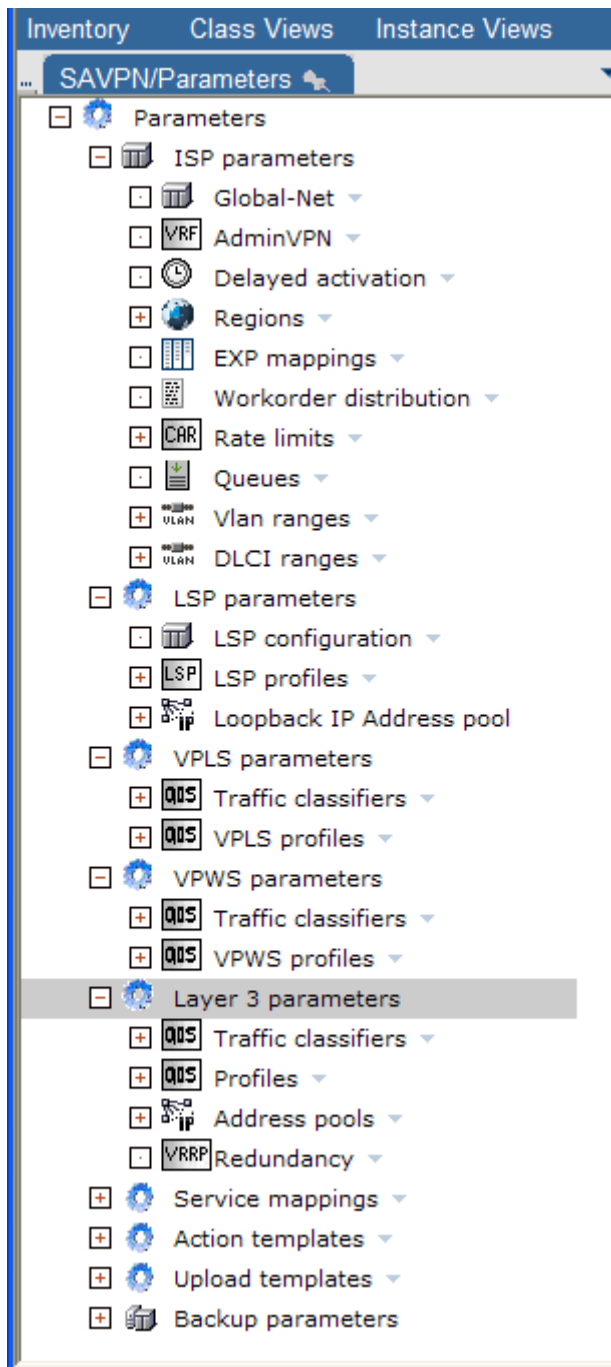
4   Service Order Management

The CRM portal enables you to enter and maintain your customer records such as customer name and address, their contact person's e-mail address and telephone number in addition to the management of customer service orders in an interactive manner. Alternatively, service orders can also be managed using flow-through activation mechanism without any operator intervention.

The main purpose of of CRM portal is for entering customer services orders and viewing and modifying the services activated for a given customer as well as monitoring the progress of new activations. The focus of the sections 4-1 through 4-5 of this chapter is customer management while the next three chapters focus on the service order management in an interactive manner.

The section 4-6 of this chapter mainly focuses on the service order management using the flow-through activation mechanism. Refer chapter 4 of *ADM* for more details on flow-through activation and northbound interface architecture and functionality.

4-1 Enter New Customer

Follow these steps to enter a new customer.

- Select the *CRM portal* from the *Tools* menu
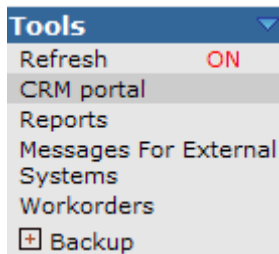
- This will open the *CRM Portal* in a separate window being logged in as the current user.
- Select *New Customer* from the *Customers* menu in the left navigation pane.

- This will display the *Create New Customer* form.

Create New Customer

Customer id	21	Unique customer identifier
Company name	Giga-trnics Inc.	Name of the company
Company address	4650 Norris Canyon Road	Company address, both street and number
City	San Ramon	The city in which the company is located
Zip code	CA 94583	Postal code
Contact person First name	John	First name of the contact person
Contact person Surname	Smith	Surname of the contact person
Phone number	328-4650	Phone number of the contact person
E-mail address	info@gigatronics	E-mail address of the contact person

- Once in the *Create New Customer* form, complete these fields:
  Customer id is provided by the system, **Company Name**, **Company Address**, **City**, **Zip Code**, **Contact person's name**, **Phone number** and **E-mail address**
- When finished, select the **Submit** ⊡ button in the bottom right hand corner of the form. This will save the records and display the *Customers* form listing the customers existing in your system.

4-2 View and Modify Customer Records

The *Customers* form allows viewing and modifying customer records as well as deleting them. From this form, you can also view the services already available for a customer.

Follow these steps to view or modify your customer records.

- Select *List* from the *Customers* menu in the navigation pane to display the *Customers* form.

Customers
New customer
List
Search

- Select the *Modify Customer* 👤 icon next to the customer whose records you want to view or modify. This will open the *Update Customer* form where you can change customer records.

Update Customer

Customer id	21	Unique customer identifier
Company name	Giga-tronics Inc.	Name of the company
Company address	4650 Norris Canyon Road	Company address, both street and number
City	San Ramon	The city in which the company is located
Zip code	CA 94583	Postal code
Contact person First name	John	First name of the contact person
Contact person Surname	Smith	Surname of the contact person
Phone number	328-4650	Phone number of the contact person
E-mail address	info@gigatronics	E-mail address of the contact person

- When finished, select the **Submit Data** ➡ button to save any changes.

4-3 Search for Customer Records

The CRM Portal allows searching for customer records. Note that the system does not require customer names to be unique. This is why it may be useful to search the customer list for existing customer records before entering a new customer to ensure that the new entry will not duplicate the existing records.

Follow these steps to search for customer records.

- Select **Search** from the *Customers* menu in the navigation pane.

Customers
New customer
List
Search

- This will display the *Search for Customers* form.
- Enter as many search criteria as necessary and select the **Search** ➡ button to submit your query. The results will be summarized in the *Search Results* form. Note that submitting a query without any criteria will return the complete list of customers entered in the system.

Search for Customers

Customer id	
Company name	
Company address	
City	
Zip code	
Contact person First name	
Contact person Surname	
Phone number	
E-mail address	
Status	⊙ Active ○ Deleted
Has pending jobs	⊙ Yes ○ No
MatchCase	○ Yes ⊙ No
	→

- In the Search Results form, you can view the services activated for a customer by selecting the Show Service ⚙ icon. You may also update (by selecting the Modify Customer 👤 icon) or delete customer records (by selecting the Delete Customer 👤 icons, see section 4-4).

4-4 Delete Customer Records

The *Delete Customer* 👤 icon is used to delete customer records but only if there are no services activated. In case a customer has services enabled, those services have to be deleted first to enable deletion of customer records. Before customer records are deleted, a warning message appears informing that you are about to delete customer records. Select **OK** to confirm delete action.

Deleted customers are kept in the database however, and may be reactivated again. The list of deleted customers may be displayed by selecting the *Status* option *deleted* in the *Search for Customers* form.

To reactivate a deleted customer, follow these steps

- Navigate to the *Customers* form
- Select **Search** and select the Status option deleted in the Search for Customers form
- In the result list select the **Modify Customer** 👤 icon.
- The customer record is activated again by selecting the *Status* option *Active* and **Submit** → button

To delete customer records permanently follow these steps.

- Navigate to the *Customers* form
- Select **Search** and select the **Status** option *Deleted* in the *Search for Customers* form.
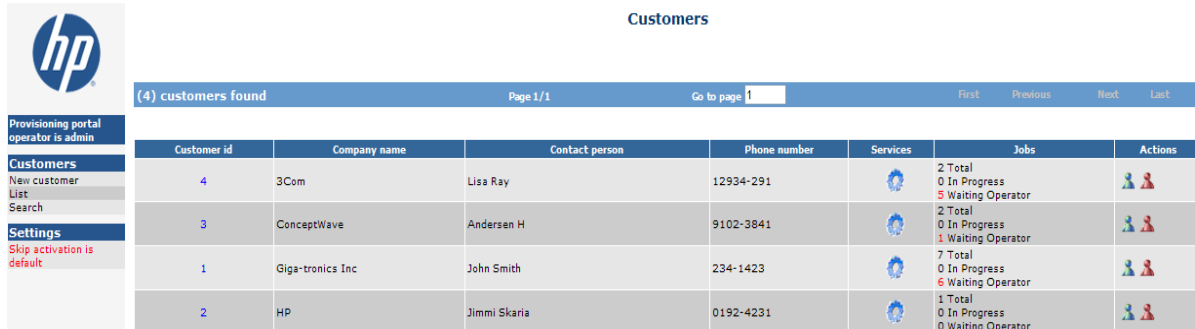
- In the result list select the *Delete Customer* ![icon] icon. The customer record will be permanently deleted from CRM Portal database.

4-5 View Active Services

Follow these steps to view the services already available for a customer.

- Select **List** from the *Customers* menu in the navigation pane to display the *Customers* form or use a *Search* (see 4-3) to get a more manageable list to select from

Clicking on List displays all the existing customers and the state of their various services.

The 'Jobs' column gives a summary of the states of various service requests requested by the customer, represented by 'Company Name'.

- Select the **Show Service** ![icon] icon next to the customer whose active as well as pending services you want to view. This will display the services (if any) already available for the customer. You will see the names and types of services that have been activated, the dates when service activation requests were submitted as well as the state of each activation request.

Few states of a service are

Ok – The service is created successfully

PE Waiting Operator – Job is waiting in the queue for operator interaction. For example, the L2 VPLS service creation waits in add_l2_site job queue, VPWS service creation waits in add_l2_vpws_site job queue and L3 service creation waits in add_l3_site_pe job queue.

PE Temporary Failure – The service activation failed because of some reason. In this case, the job waits in the Failed_Jobs queue for operator to resolve and resubmit the service request, or to fail the operation.

Modify PE Wait Start Time – When the service is planned for activation at a scheduled time.

4-6 Service Order Management through FTA

The term "flow-through activation" in the service fulfillment parlance generally refers to end-to-end fulfillment, beginning with service order entry and concluding with service activation of network elements. An order management operator records the order, and all corresponding workflow activities and associated tasks are subsequently completed without any human intervention. The term FTA refers to flow-through activation through out the document in general.

4-6-1 Pre-requisites

VPN_SVP operating in FTA mode doesn't remove the requirement/need of having the Equipment Tree populated with the requested TP resources. One of the main pre-requisites prior to the service orders management though FTA or otherwise is the population of Network Elements, in the inventory. This can be achieved either through the process of manual creation using inventory as described in chapter 3 or though the import utility [refer section 11-2 for more details on XML import utility] or through the NNMi dataload process [refer chapter 12 for more details on dataload using NNMi].

4-6-2 FTA Requests

Operators can submit service order request using FTA mode via the NBI provided by VPN_SVP (refer *ADM* for the details on the format of service order requests and responses). Whether a submitted request is to be treated like an FTA or non-FTA request is determined by the value of FTA attribute in the service header. The presence of this attribute and value of this attribute being set to 'true', indicates that, the request message has to be treated in FTA mode. In case this attribute is absent in the service header or the value of this attribute is set to 'false' – the request would be treated like a non-FTA or an interactive request.

4-6-3 Error Handling

For the service order requests submitted in FTA mode, the interactive problem control described in section 10-1 and 10-2 is eliminated. In FTA mode problem control and management is assumed performed separately from the activation process. To ease this process the service order response messages includes extensive information about the nature and cause of the problem. Refer to *ADM* section 4-4 for more details on the formats and contents of the response messages.

4-6-4 Service Order Requests using FTA

The complete details on request/response message format to be sent or received from VPN_SVP NBI can be found in chapter4 of ADM. As already explained in the section 3.2 of *ADM* several types of requests are by nature Flow-through and do not need any further information to be provided by the network operator to complete irrespective of the Activation mode. These include Creation/Deletion of VPNs and VPN Sites, Modifications of existing services attachments, Enabling/Disabling of existing services and Removal of existing services. While the other services like addition of an attachment require the inclusion of resources block/s in their requests.

5   Layer 2 VPN Services

The CRM Portal enables delivery of Layer 2 VPN (Virtual Private LAN Service or VPLS) services to a customer.

Service delivery in CRM portal sums up to:

- CRM order operator locates customer in portal, optionally creates customer.
- Selecting layer2-VPN service creation for customer.
- Adding customer layer2-VPN sites to VPNs where the service is required.
- Entering customer specific service parameters into form.
- Submitting service request to HPSA (and the network operator).

Service Activation in HPSA portal requires the network operator to complete these tasks:

- Interacting with a job,
- Selecting Edge-router and port/interface for service attachment.
- Submitting the selection to let HPSA configure the network for service delivery.

5-1 Layer 2 VPN Service Request in CRM Portal

5-1-1 Enable Layer 2 VPN Service

Follow these steps to create a Layer 2 VPN service for a customer.

- Log in to CRM portal.
- Search for the customer for which a service has to be added. (See 4-3 Search for Customer Records for instructions.) Below is assumed that customer *Giga-Tronics Inc.* is selected.

- Once the search results are displayed, select the *Show Services* icon next to the required customer. The *Customer Services* form will open showing the services (if any) activated earlier.

- To add a Layer 2 VPN service, select the *Layer2-VPN* icon in the *Create New Services* region. This will open the *Create Service* form.

Complete the service parameters:

- Layer2 VPN Service ID is provided by the system.
- Enter the name of the service in the **VPN Name** field: *Financials*.
- From the drop-down list, select a value for the **interface type** field. In this scenario select *port-vlan.* Available options include *port*, and *port-vlan.*

NOTE: The customer may choose between the two different UNI types, i.e. *port* and *port-vlan.*

If the option *port* is selected, your customer will exclusively use a full port on an access device. The service provider will ensure that all L2 packets from one port will be forwarded to other L2 sites within the VPN. This corresponds to the MEF service type EP-LAN (Ethernet Private LAN, see **Table 2-2**).

If the option *port-vlan* is selected, your customer may share a port with many other users or with other services from the same customer site. The customer's traffic will be VLAN tagged before reaching the router to distinguish it from data from other services and/or from other users. All the L2 packets bearing the specific VLAN tag will be forwarded to other sites within the same VPN. This corresponds to the MEF service type EVP-LAN (Ethernet Virtual Private LAN).

In some cases, the traffic is not tagged from the customer site but a Multiplex unit may be inserted between the customer's LAN and the access device. The Multiplex unit has to be configured to tag all traffic with the given VLAN tag that is also to be used when creating the service.

Within a VPN it is currently not possible to mix port and *port-vlan* interface types. If a VPN is of the *port-vlan* type, then all the sites within the VPN must be of the *port-vlan* type.

If the UNI type *port* is selected, the encapsulation used on the access device will be QinQ (802.1ad). This means that a provider (or service) Vlan tag will be added at the access port. When the access device is an access switch in an access network, this service Vlan id will be used to setup the attachment of the service from the UPE port to the N-PE port. The Inner customer specific Vlan tags will not be visible or available for the activation of the service.

If the UNI type *port-vlan* is selected, the encapsulation used on the access device will be Vlan tagged (802.1q).

- If the *port-vlan* **interface type** is selected, it informs VPN_SVP that the customer traffic for sites in this VPN will be VLAN tagged. You will be prompted to select *Enabled* or *Disable* option for the **Fixed Vlan id** field.

Enabling the **Fixed Vlan id** option informs VPN_SVP that all sites belonging to this *port-vlan* mode VPN will by default be configured to use the *same* VLAN tag. This tag may be entered in the **VLAN id** field (Customer selected) or the field may be left blank which indicates that the Provider will select a common value (Provider selected).

NOTE: When the service is attached via an access network, the **Fixed Vlan id** option allows multiple sites using the same Vlan id to be attached via the same access network (N:1 allocation). Hence, inter-site traffic may be switched directly in the access network between sites in the Layer2 VPN and not reach the N-PE router. The VPN_SVP does not currently support means for specifying Private Vlan ids or other means to isolate the traffic among ports using the same Vlan id within an access network.

Disabling the **Fixed Vlan id** option informs VPN_SVP that the routers may be configured to use different VLAN ids for the customer traffic on different sites (which supports **Vlan mapping**).

NOTE: Even when the Fixed Vlan id option have been selected, it will still be possibly to select a different Vlan id when provisioning the site service (**Vlan mapping**)

- Select a value for the **QoS Profile** field from the drop down list. This value represents the default site value when sites are being added.
- In the field **Comments**, you may add any service related notes, which will be forwarded to the Service Activator and will be visible and possibly useful to the Network Operator throughout the further activation process.

NOTE: The values **VLAN id** and **QoS Profile**, will be defaulted for all new sites added to the VPN.

- Select the **Submit** button in the bottom right hand corner of the form to proceed. An XML message with the specified service parameters will be forwarded to Service Activator. You will be returned to the *Customer Services* form where you will find the newly defined service.

From this point, the new VPN service is visible in the HPSA inventory. You may log in to Service Activator and navigate to the *Inventory GUI's SAVPN/ Services view* to verify. (See section 5-3-1 for detailed instructions.)

5-1-2 Add Layer 2 VPN Sites

Sites can now be added to your Layer 2 VPN Service created in 5-1-1 Create Layer 2 VPN Service. Follow these steps to add a site to the VPN service.

- Navigate to the *Customer Services* form.
- Locate the newly created Layer2 VPN '*Financials'* in the *Existing Services* section
- Select the **Submit** button in the *Existing Services* with **Type** *'layer2-VPN'* and **Name** '*Financials'*, to requests a **Subservice** of type '*layer2-Site*' as indicated in the form.

Enter the L2 site-level parameter details in the *Create service* form:

- Layer2-VPN id and **layer2-Site id** are auto-allocated by the CRM system.
- Enter the name of the site in the **site name** field. In this example this is entered as *Headoffice*.

NOTE: The **site name** field may be entered in two ways: As an operator specified string in case of a new site is to be created or by selecting an existing site name from the drop-down list.

When a new site name is entered, the site will be automatically created as part of the request submitted to HPSA before the requested service then gets associated the site.

When an existing site is selected, the service will be added to the existing services, by using a service specific Vlan id on the access port that previously was chosen when the selected site was created. This is referred to as service multiplexing.

Not all combination of site services is permitted. Basically the existing site services, as well as the new service, must be port-vlan based.

The CRM Portal does not keep the detailed network information and may not in all cases be able to validate directly, if the selected service may be added using the specified Vlan id. As part of handling the request in HPSA when it is submitted, a service validation (or feasibility check) will be performed. If the check indicates that the new service may not be added to the existing site, a REUSE error will be raised.

- Select the value 'North-East' for the field *Region* from the drop-down list and *Location* 'Metropol North-West'. These values indicate the region in the provider's network which includes this customer site and the location limits the selection of PE routers that will be used to provide the service for this site.

NOTE: The VPN_SVP can only deliver Layer 2 VPN services on routers that support the VPLS functionality. But both rfc4761 and rfc4762 types of VPLS functionality is supported. The PE router attribute **BGPDiscovery** selects rfc4761 behavior. See e.g. section 3-5 .

- Even if the layer2 VPN was created with **Fixed VLAN id** enabled, it will be possible on a per site basis to override this by enabling **VLAN mapping**. When **VLAN Mapping** is *Enabled* a **VLAN id** entry field appears. Here the desired (Customer selected/agreed) VLAN tag may be entered or if it is left blank, a provider selected value will be used. Provider selected VLAN tags tend to be fixed (i.e. equal) for all sites of the VPN.

- From the drop-down list, select a value for the **rate limit** field. This value represents the total bandwidth allocated for this site attachment.

- From the drop-down list, select a value for the **QoS profile,** e.g. the *L2_STD_20.20.20.20.20* VPLS profile. The profile specifies how the selected bandwidth will be distributed among 5 CoS (each gets 20%). The classification is based on the IEEE 802.1p bits and is defined in the *Inventory SAVPN/Parameters* view*, VPLS parameters* section.

NOTE: QoS configuration is used to provide differentiated treatment of the traffic being exchanged between the provider network and the customer site.

VPN_SVP supports up to 8 classes of services (CoS). The VPN_SVP QoS components consist of Traffic classifiers and Profiles. The QoS profiles use the following naming convention

<center><name>_p1.p2.p3.p4.p5.p6.p7.p8</center>

where the p1,..,p8 are values from 0-100 that represents the percentage of the requested rate limit allocated each of up to 8 CoS. The sequences of CoS are as specified in the *EXP mappings* table in *SAVPN/Parameters*. E.g. with 5 CoS defined, the EXP mappings could be

Class Name	MPLS EXP	CE DSCP	Loss Priority	Queue
Best-Effort	1	8	high	bronze
Bronze	2	16	low	bronze
Silver	3	24	low	silver
Gold	4	32	high	gold
Platinum	5	40	low	gold

and the percentages would correspond to

p1 ~ Best-Effort

p2 ~ Bronze

p3 ~ Silver

p4 ~ Gold

p5 ~ Platinum

and p6, p7and p8 will not be specified.

Hence, e.g. the profile *L2_STD_20.20.20.20.20* associates 20% of the customer traffic with each of the above 5 CoS.

The QoS profiles implements rate limiting of ingress traffic and shaping of egress traffic on the Provider edge device.

Traffic classifiers determine which class data traffic belongs to. The techniques for this may be quite varied from simply stating that all traffic belongs to a specific class, to inspecting each and every packet and classify these individually (often implemented in router hardware).

VPN_SVP QoS supports configuration of the L2 classification based on 802.1 p-bit values (also called CoS bits). The p-bit based classification allows you to specify a list of values (e.g. 4,5).

When the data traffic is forwarded into the MPLS core network, the CoS of the packet determines the EXP bit value the MPLS packet will be marked with. This value is selected from the *EXP mappings* table MPLS EXP column and is made part of the QoS profile configuration. From here it is included by VPN_SVP as part of service activation.

- The *Create service* form includes a **Scheduling information** section. Most service requests may be requested as *timed services* for which a **start time** and optionally an **end time** may be specified. Leaving the **start time** empty means that the service request should be processes immediately; leaving the **end time** empty means the service should stay activated (until otherwise terminated by operator).

Service information	
VPN name (id)	Financials (1020)
layer2-Site id	1022
site name	Headoffice ▼
region	Denmark ▼
location	Copenhagen ▼
VLAN mapping	⦿ Enabled ○ Disabled
VLAN id	

Parameters for QoS		
rate limit	2M ▼	
QoS profile	L2_STD_20.20.20.20.20 ▼	
Best-Effort	l2_any	20 ▼
Bronze	l2_bronze	20 ▼
Silver	l2_silver	20 ▼
Gold	l2_gold	20 ▼
Platinum	l2_platinum	20 ▼

Scheduling information		
start time		▦ Reset
end time		▦ Reset

Comments

→

- Select the **Submit** → button to forward the site service request to Service Activator. You will be returned to the *Customer Services* form where you will find the new site added to the VPN service. The form allows monitoring the progress of site-level activation.

57

Id ▲	Name	State	Type	Submit date	Action	Subservices	
1037	Financials	Ok	layer2-VPN	13/11/2010	↺✕	layer2-Site ▾	➜
⊟ 1038	Headoffice	Ok	Site	13/11/2010	None	*No subservices*	
1039	-	PE Waiting Operator	layer2-Attachment	13/11/2010	None		

Existing services (7) — Page 1/1 — Go to page 1 — First Previous Next Last

NOTE: The CRM portal keeps the **State** of a service updated in the *Customer services* view:

- *Request Sent* - Indicates that an activation request has just been issued and sent to Service Activator.

- *In Progress* - Indicates that the activation request is being process in Service Activator.

- *PE Waiting Operator* – Indicates that the activation request is waiting for the network operator interaction on HPSA and this State could persist for a considerable time.

- *OK* - Indicates that the activation has been completed.

- Failures will initially be handled by the network operator on HPSA using the ErrorHandler. Failed services will be in state *Temporary Failure* with n*o* **Actions** available. See chapter 10-2 for further information.

Having requested the customer's site service, the network operator takes over the request and uses Service Activator to perform the activation tasks. See 5-2-1 Activate PE Router for Layer 2 Service.

5-2 Layer 2 VPN Site Service Activation in HPSA

5-2-1 Activate PE Router for Layer 2 VPN Site Service

The service request for the new site has now been received on HPSA. The request is posted on the *add_l2_site* job queue. To deliver the L2 service, an operator must then interact with the job, select the router and port for the service and physically connect the router.

If you can not locate the job in the *add_l2_site* queue, please see the note on regions and roles in section 0.

Follow these steps to activate your PE router for the service requested in 5-1-2 Add Layer 2 VPN Sites:

- Log in to Service Activator. Make sure your role will match the region '*North-West*' selected for the request

- Select *Jobs* from the *Work Area* menu in the left navigation pane. This will display the *Active Jobs* form.

- Select the *add_l2_site* job queue.

- Select and right-click the job to interact with. This will open a pop-up menu.

Active Jobs

- Select *Interact with Job* from the additional menu.
- Select a router in the location of the customer's site (only the routers located in the location will be available in the drop-down list).
- Select one of the free ports on the router (only free ports will be available in the Select Port drop-down list)

In practice, an operator could now attach the cables that connect the customer site to the selected port or assure that this has been completed, and select the **Submit** button. Service Activator will proceed to activate and configure the selected port of the router.

NOTE: Ports which are already in use for Layer 2 port services are not listed in the drop-down list for the **Select Port** field. Furthermore, if a customer has requested a port-vlan service, then only the ports where the selected VLAN tag is not already in use will be listed.
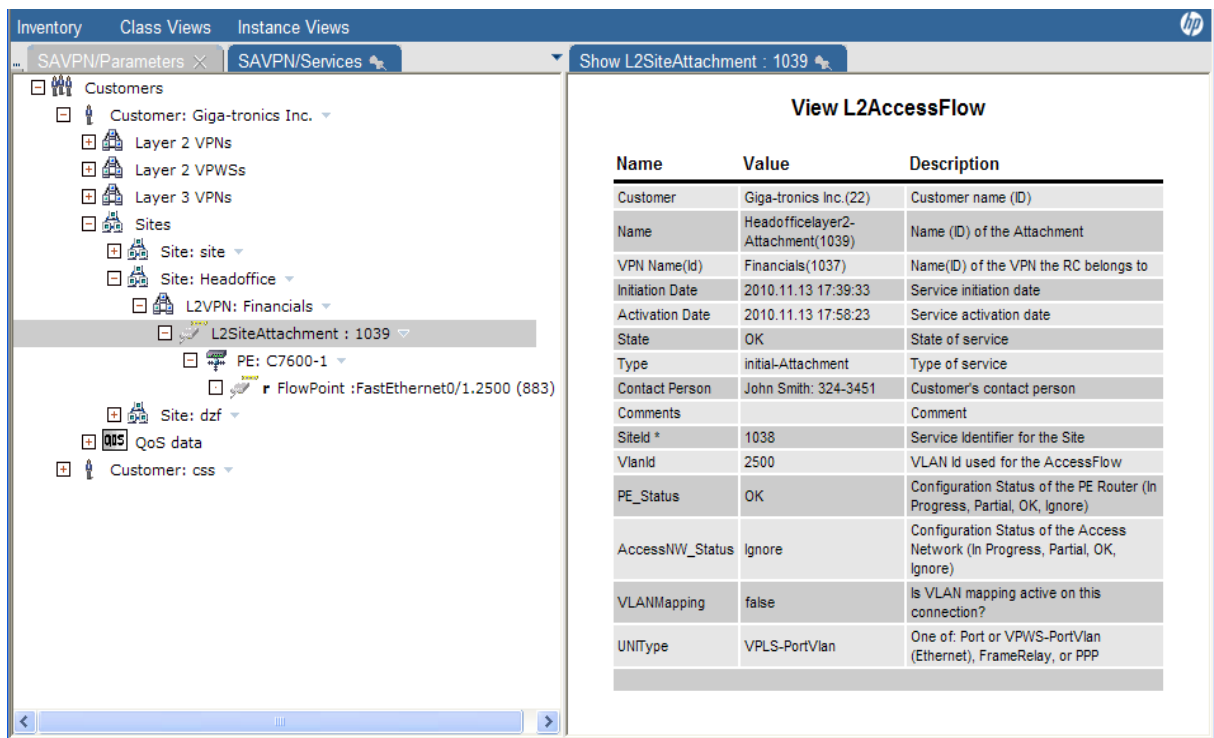
5-3   View and Modify Layer 2 VPN Site Service

5-3-1   View Layer 2 VPN Site Service in HPSA Inventory

Once the new service has been successfully delivered, it is possible to locate the service in the HPSA inventory GUI.

- Log in to Service Activator.
- Navigate to the *Inventory GUI* window and select the *SAVPN/Services* view.
- Expand the *Customers* branch to locate your customer *Giga-tronics Inc.*
- Expand the *Giga-tronics Inc.* branch to view the VPN services.
- Expand the S*ites* branch to view the sites and its service parameters.
- Expand the *Headoffice* site
- Expand the *L2VPN: Financials* branch
- Select View on the *L2SiteAttachment* object

The service related parameters are displayed:

.

5-3-2   Modify Layer 2 VPN Site Attachment Service in CRM Portal

Services can be modified in CRM Portal. In the example below, *Rate Limit* of the Layer 2 site created in 5-1-2 Add Sites is changed.

- Log in to CRM Portal.
- Find your customer *Giga-tronics Inc.* and open the *Customer Services* form. (See also 4-3 Search for Customer Records for navigation instructions).

● In the *Existing* Services region of the *Customer Services* form, select the *Modify Service* icon next to the site 'Headoffice' you intend to update. This will open the *Modify Layer2-Attachment* form.

Modify layer2-Attachment

Customer id	Company name	Contact person	Phone number	E-mail address	Services
21	Giga-tronics Inc.	John Smith	328-4650	info@gigatronics.com	

Service information	
layer2-AttachmentId	Headofficelayer2-Attachment (1023)
parameter to modify	Modify QoS
	Select modify...
	Modify QoS

● To modify the site rate limit, select *Modify QoS* from the drop-down list for the field **Parameter to modify**.

● Select a new rate limit for the site from the drop-down list. In the *Scheduled Activation Time* field, it is possible to indicate the time when the change should take place. Leave the field blank to get immediate activation.

Service information				
layer2-AttachmentId	Headofficelayer2-Attachment (1039)			
parameter to modify	Modify QoS			
rate limit	10M			
	128K			
	256K			
	512K	20.20.20.20.20		
QoS profile	1M			
Best-Effort	2M	20	2Mbps	
Bronze	10M	20	2Mbps	
Silver	144M	20	2Mbps	
Gold	l2_gold	20	2Mbps	
Platinum	l2_platinum	20	2Mbps	
Scheduling information				
start time		Reset		
end time		Reset		
periodic?	No			
repeat	Daily			
until		Reset		

● When complete, choose the **Submit** button.

Your site modify request will be forwarded to Service Activator. The request will start a workflow which will handle the request and manage the router activation to deliver the requested service. No

further operator interactions is necessary as all required parameters are know, either from the request message or from the Inventory of the existing service.

To view the result of site modification:

- Log in to Service Activator.

- Navigate to the *Inventory GUI* window.

- Select the *SAVPN/Services* view and expand the *Customers* branch.

- Locate your customer and expand its branch.

- Expand the *Sites* branch.

- Select and expand the site which was modified in 5.4.2 Modify Service in CRM Portal.

- Expand the *L2VPN: Financials* branch to which the site was added

- Select the *L2SiteAttachment* to view the generic parameters like Vlan id.

- Expand the *L2SiteAttachment branch* to see the PE router onto which this service is attached.

- Expand the PE router branch (*PE: C7600-1*) and select the Flowpoint of the service. The new rate limit will be displayed in the *Rate_Limit* lines.

6 Layer 2 VPWS Services

The CRM Portal enables delivery of Layer 2 VPWS (Virtual Private Wire Service or Point-to-Point) services to a customer.

Service delivery in CRM portal sums up to:

- Optionally creating and locating the customer in portal.
- Selecting layer2-VPWS service creation.
- Entering customer specific service parameters into form.
- Submitting service request to HPSA (and the network operator).

Service Activation in HPSA portal requires the network operator to complete these tasks:

- Interacting with a job.
- Selecting Edge-router and port/interface for service attachment.
- Submitting the selection to let HPSA configure the network for service delivery.

6-1 Layer 2 VPWS Service Request in CRM Portal

6-1-1 Enable Layer 2 VPWS Service

Follow these steps to create a Layer 2 VPWS service for a customer.

- Log in to CRM portal.
- Search for the customer for which a service has to be added. (See 4-3 Search for Customer Records for instructions.) Below is assumed that customer *Giga-tronics Inc.* is selected.
- Once the customer search results are displayed, select the *Show Services* icon next to the required customer. The *Customer Services* form will open showing the services (if any) activated earlier.
- To add a Layer 2 VPWS service, select the *Layer2-VPWS* icon in the *Create New Services* section. This will open the *Create Service* form.

VPWS services are characterized by interconnecting exactly two sites, aEnd and zEnd. Hence, the form requires the VPWS service name and the two sites names to be provided.

Complete the service parameters:

- Layer2 VPWS Service ID is provided by the system.
- Enter the name of the service in the **VPWS Name** field: *CPH-STK*
- Select a **QoS profile** from the drop-down list. For VPWS only a single CoS is supported. E.g. select vpws_0.0.0.100.0 to select Gold class.

Service information	
layer2-VPWS id	1042
VPWS name	CPH-STK
rate limit	2M
QoS profile	vpws_0.0.0.0.100
Platinum	vpws_any 100 2Mbps

Site information	aEnd	zEnd
site name	Copenhagen	Stockholm
site service id	1043	1045
site attachment id	1047	1048
interface type	Ethernet	Ethernet
service type	port	port
region	Denmark	Sweden
location	Copenhagen	Stockholm

Scheduling information		
start time		Reset
end time		Reset

Comments

NOTE: QoS configuration is used to provide differentiated treatment of the traffic being exchanged between the provider network and the customer site.

VPN_SVP supports up to 8 classes of services (CoS). The VPN_SVP QoS components consist of Traffic classifiers and Profiles. The QoS profiles use the following naming convention

   <name>_p1.p2.p3.p4.p5.p6.p7.p8

where the p1,..,p8 are values from 0-100 that represents the percentage of the requested rate limit allocated each of up to 8 CoS. The sequences of CoS are as specified in the *EXP mappings* table in *SAVPN/Parameters*. E.g. with 5 CoS defined, the EXP mappings could be

Class Name	MPLS EXP	CE DSCP	Loss Priority	Queue
Best-Effort	1	8	high	bronze
Bronze	2	16	low	bronze
Silver	3	24	low	silver
Gold	4	32	high	gold
Platinum	5	40	low	gold

and the percentages would correspond to

- p1 ~ Best-Effort

- p2 ~ Bronze

- p3 ~ Silver

- p4 ~ Gold

- p5 ~ Platinum

and p6, p7and p8 will not be specified.

Hence, e.g. the profile *vpws_0.0.0.100.0* associates 100% of the customer traffic with the Gold CoS. The VPWS QoS profiles implements rate limiting of ingress traffic.

Multiple CoS can not currently be associated a VPWS service. Currently only a single CoS is supported which may be any one of the defined CoS. This means that all traffic from the customer site belongs to a single specific CoS, As all traffic is associated a single CoS no classification is required. Hence all traffic (100%) is associated a dummy vpws_any classification.

When the data traffic is forwarded into the MPLS core network, the CoS of the packet determines the EXP bit value the MPLS packet will be marked with. This value is selected from the *EXP mappings* table MPLS EXP column and is made part of the QoS profile configuration. From here it is included by VPN_SVP as part of service activation.

- Select the **rate limit** from the drop-down list
- Enter the **site name** for aEnd and for zEnd, e.g. *Copenhagen* and *Stockholm*

NOTE: The **site name** field may be entered in two ways: As an operator specified string in case of a new site is to be created or by selecting an existing site name from the drop-down list.

When a new site name is entered, the site will be automatically created as part of the request submitted to HPSA before the requested service then gets associated the site.

When an existing site is selected, the service will be added to the existing services, by using a service specific Vlan id on the access port that previously was chosen when the selected site was created. This is referred to as service multiplexing.

Not all combination of site services is permitted. Basically the existing site services, as well as the new service, must be port-vlan based.

The CRM Portal does not keep the detailed network information and may not in all cases be able to validate directly, if the selected service may be added using the specified Vlan id. As part of handling the request in HPSA when it is submitted, a service validation (or feasibility check) will be performed. If the check indicates that the new service may not be added to the existing site, a REUSE error will be raised.

- The layer2 VPWS **site service id** are provided by the system
- From the drop-down list, select a value for the **interface type** (or UNI type) for each of the two sites. In this scenario select *Ethernet.* Available options include *Ethernet, FrameRelay* and *PPP.*
- For **interface type** *Ethernet*, two service types may be selected, *port* and *port-vlan.* If **service type** *port-vlan* value is selected, it informs VPN_SVP that the customer traffic for the two sites in this VPWS will be VLAN tagged. Enter the Customer **VLAN Id** or leave the **VLAN Id** field empty to let the VPN_SVP configure a provider allocated valued.
- For **interface type** *FrameRelay,* a customer **DLCI** value must be entered or leave the **DLCI** field empty to let the VPN_SVP configure a provider allocated valued.

NOTE: For Ethernet interfaces, the customer may choose between the two different types of services, i.e. *port* and *port-vlan.*

If the option *port* is selected, your customer will exclusively use a full port on an access device. The service provider will ensure that all L2 packets from one port will be forwarded to the other site in the VPWS.

If the option *port-vlan* is selected, your customer may share a port with many other users. The customer's traffic must be VLAN tagged before reaching the access device to distinguish it from other users' traffic. All the L2 packages with this specific VLAN tag will be forwarded to the other site in the same VPWS.

Within a VPWS it is not possible to mix both *port* and *port-vlan* **service types**.

The following combinations of heterogeneous service types are supported (if the vendor equipment otherwise supports it):

> Eth Port↔Eth Port
>
> Eth PortVlan↔Eth PortVlan, FR, PPP
>
> FR↔Eth PortVlan, FR, PPP
>
> PPP↔Eth PortVlan, FR, PPP

- Select the value 'Denmark' and 'Sweden' for the field **region** from the drop-down list and **location** 'Copenhagen' and 'Stockholm' (assuming that these regions and locations have been created as described in section 1-1). These values indicate the region in the provider's network which covers the customer site and the location limits the selection of PE routers that will be used to provide the VPWS service, to that location (or POP).

- In the field **Comments**, you may add any service related notes, which will be forwarded to the Service Activator and will be visible to the Network Operator throughout the process of activation.

- The *Create service* form includes a **Scheduling information** section. Most service requests may be requested as timed services for which a **start time** and optionally an **end time** may be specified. Leaving the **start time** *empty* means that the service request should be processes immediately; leaving the **end time** *empty* means the service should stay activated

- Select the **Submit** button in the bottom right hand corner of the form to forward the site service request to Service Activator. An xml message with the selected service parameters will be forwarded to Service Activator. You will be returned to the *Customer Services* form where you will find the newly defined service being *In Progress*.

Existing services (8)		Page 1/1		Go to page 1	First Previous Next Last		
	Id ▲	Name	State	Type	Submit date	Action	Subservices
	1042	CPH-STK	Waiting Operator	layer2-VPWS	13/11/2010	None	
⊟	1045	Stockholm	Waiting Operator	Site	13/11/2010		
	1048	-	PE Waiting Operator	vpws-Attachment	13/11/2010		
⊟	1043	Copenhagen	Waiting Operator	Site	13/11/2010		
	1047	-	PE Waiting Operator	vpws-Attachment	13/11/2010		

- The form allows monitoring the progress of the site-level activation.

- When requesting a service where a new site is specified (and not an existing site selected) an create site request is automatically submitted before the request for the service specific site attachment is submiited.

NOTE: The CRM portal keeps the **State** of a service updated in the *Customer services* view:

- *Request Sent* - Indicates that an activation request has just been issued and sent to Service Activator.

- *In Progress* - Indicates that the activation request is being process in Service Activator.

- *PE Waiting Operator* – Indicates that the activation request is waiting for the network operator interaction on HPSA and this State could persist for a considerable time.

- *OK* - Indicates that the activation has been completed.

- Failures will initially be handled by the network operator on HPSA using the ErrorHandler. Failed services will be in state *Temporary Failure* with n*o* **Actions** available. See chapter 10-2 for further information.

Having requested the customer's VPWS service, the network operator takes over the request and uses Service Activator to perform the activation tasks. See 6-2-1 Activate PE Router for Layer 2 VPWS Service.

6-2 Layer 2 VPWS Service Activation in HPSA

6-2-1 Activate PE Router for Layer 2 VPWS Service

The service request for a VPWS service has now been received in Service Activator. The request is posted on the *add_l2_vpws_site* job queue. To deliver the L2 VPWS service, a network operator must interact with the job for the aEnd; select the router and port for attachment of this site service.

Following this, a network operator must then interact with the job for the zEnd, select the router and port for that service. It is assumed that the customer sites are physically attached to the respective Edge devices.

Follow these steps to activate your PE router for the service requested in 6-1-1 Enable Layer 2 VPWS Service:

- Log in to Service Activator; if you login as user 'dk, your role will match the region 'Denmark' selected for the aEnd part of the request

- Select *Jobs* from the *Work Area* menu in the left navigation pane. This will display the *Active Jobs* form.

- Select and right-click the job to interact with. This will open a pop-up menu.

- Select **Interact with Job** from the pop-up menu.

- Select a router in the customer site region (only the routers located in the region will be available in the drop-down list).

- Select one of the available interfaces on the router.

In practice, an operator would now attach the cables that connect the customer site to the selected interface, and select the **Submit** button. Service Activator will proceed with activation and configuration of the selected interface of the router.

When the aEnd has been completed as described above, the zEnd job will appear in the jobs view of operators having a role associated the corresponding region.

- Log in to Service Activator; if you login as user 'se', your role will match the region 'Sweden' selected above for the zEnd part of the request.

- Proceed as described above for the aEnd

Interact with job: L2VPWS_ReserveResource

Job ID	Workflow	Start Date & Time	Post Date & Time	Step Name	Description	Status
108378	L2VPWS_ReserveResource	Sat Nov 13 18:25:23 IST 2010	Sat Nov 13 18:25:23 IST 2010	Select_router_and_port	Select router and port for the site	Running

Customer Name   Giga-tronics Inc.

VPWS Name   CPH-STK **Id:** *1042*

Site Name   Copenhagen

Requested Rate limit 2M

Router Location   Copenhagen

Region   Denmark

Select Router   Juniper-1 (PE)

Router Id   6

UNIType   Port

Select interface   fe-0/0/0

Topology view   NNM L3 Neighbor View   Launch Views

Contact Person   John Smith: 324-3451

Comment

Submit Clear

NOTE: Interfaces which are already in use for Layer 2 services are not listed in the drop-down list for the Select interface field. Furthermore, if a customer has requested an Ethernet port-vlan service, then only the interfaces where the selected VLAN tag is not already in use will be displayed.

In the case an Ethernet type of interfaces is to be selected, note that if the requested *rate limit* is less than 2Mb, interfaces with bandwidth higher than 10Mb are not displayed.
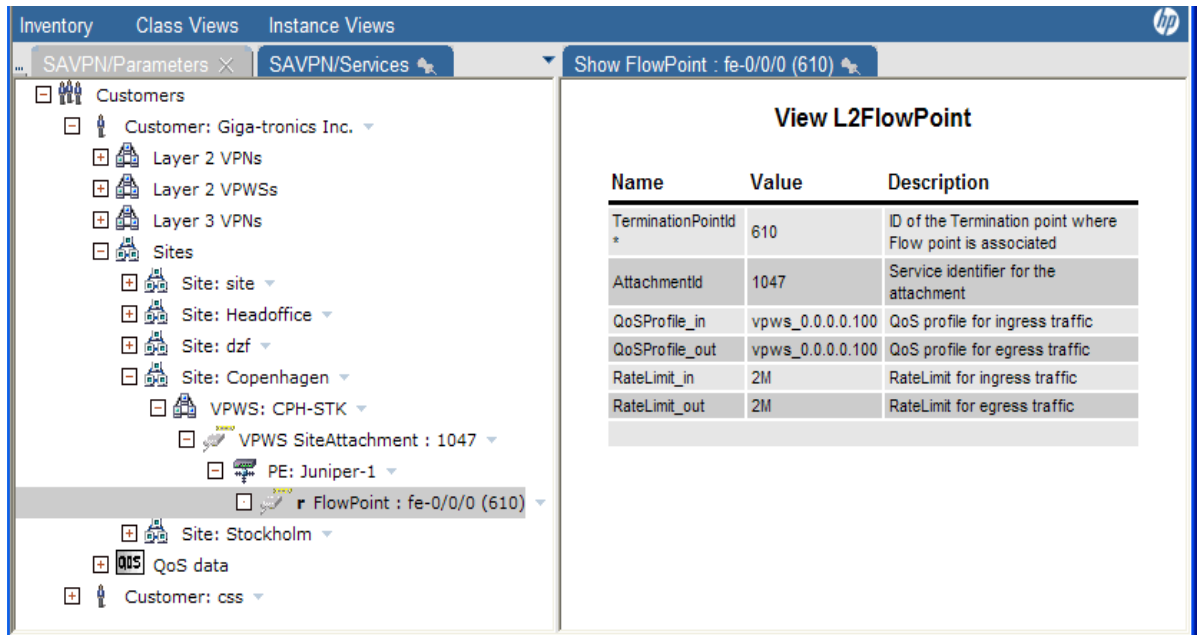
6-3 View and Modify Layer 2 VPWS Service

6-3-1 View Layer 2 VPWS Service in HPSA Inventory

Once the new VPWS service has been successfully delivered, it is possible to locate the service in the HPSA inventory.

- Log in to Service Activator.
- Navigate to the *Inventory GUI* window and select the *SAVPN/Services* view.
- Expand the *Customers* branch to locate your customer *Giga-tronics Inc.*
- Expand the *Giga-tronics Inc.* branch to view the services.
- Expand the *Layer 2 VPWS* branch
- Expand the VPWS service: *CPH-STK* and expand one of the two sites
- Select View on the Connection object

The service related parameters are displayed

6-3-2 Modify Layer 2 VPWS Service in CRM Portal

Services can be modified in CRM Portal. In the example below, *Rate Limit* of the Layer 2 VPWS site created in 6-1-1 Enable Layer 2 VPWS Service is changed.

- Log in to CRM Portal.

- Find your customer *Giga-tronics Inc.* and open the *Customer Services* form

- In the *Existing* Services region of the *Customer Services* form, select the *Modify Service* 🖉 icon next to the VPWS service 'CPH-STK' you intend to update. This will open the *Modify Layer2-VPWS form*.

- To modify the site rate limit, select *Modify Rate-limit* from the drop-down list for the field **Parameter to Modify**.

- This will open the Modify rate-limit form

- Select a new rate limit for the site from the drop-down list. In the **Scheduling information** field, it is possible to indicate the time when the activation should take place. Leave the field blank to get immediate activation.

- When complete, choose the **Submit** button.

Your request to modify the site will be forwarded to Service Activator. The request will start a workflow which will handle the request and manage the router activation to deliver the service request without the need of any network operator interactions.

To view the result of site modification:

- Log in to Service Activator, navigate to the *Inventory GUI* window and select the *SAVPN/Services* view.
- Expand the *Customers* branch to locate your customer *Giga-tronics Inc.*
- Expand the Layer 2 VPWSs branch to view the VPWS services.
- Expand the CPH-STK service and select the site which was modified in section 6-3-2
- Select View on the Connection object. The service related parameters are displayed.
- Select the L2VPWSSiteConnction *object* to view the connection parameters. The new rate limit will be displayed in the **Rate Limit** line.

7 Layer 3 VPN Services

The CRM Portal enables delivery of Layer 3 VPN services to a customer.

Layer 3 VPN Service activation in the CRM portal sums up to:

- CRM order operator locates customer in portal, optionally creates customer,
- Selects layer3-VPN service creation for customer,
- Adds customer layer3-VPN sites to VPNs where the service is required.
- Enters customer specific service parameters into forms.
- Submits service request to Service Activator (and the network operator).

Service activation in the HPSA portal requires the network operator to complete these tasks:

- Interacting with a job,
- Selecting provider Edge-router and port/interface for service attachment.
- Optionally selecting customer edge (CE) routers for managed customer sites.
- Submitting the selection to let HPSA configure the network for service delivery.

7-1 Layer 3 VPN Service Request in CRM Portal

7-1-1 Enable Layer 3 VPN Service

Follow these steps to enable Layer 3 VPN service for your customer.

- Log in to CRM portal.
- Search for the customer *Baldor Electric Company* (which we assume has already be created according to the instructions in chapter 4) for which a L3 service has to be enabled. (See section 4-3 Search for Customer Records for instructions.)
- Select the *Show Services* icon next to the selected customer. The *Customer Services* form will open showing the services (if any) activated earlier.

- To add a layer 3 VPN service, select the *layer3-VPN* icon in the *Create New Services* area. This will open the *Create Service* form.

Complete the service parameters:

- The **layer3-VPN id** is generated uniquely by the CRM portal system.
- Enter the name of the service in the **VPN Name** field: *Sales.*
- Select the **VPN topology** type from the drop-down list. Your customer requests the Hub and Spoke topology.

NOTE: VPN_SVP supports different layer3 VPN topologies: *Full mesh* and *Hub and spoke*.

Fully meshed topologies consist of sites having symmetric connectivity: Any site may communicate with any other site.

But for Hub-and-spoke topologies sites are having "anti-symmetric" connectivity: a hub site may communicate with any spoke (and possibly other hubs) but spoke sites may only communicate with the hub(s). The Hub-and-spoke topology that VPN_SVP supports is what is also known as 'Central services' topology.

Fully meshed topologies may be selected for VPNs where all sites needs to exchange information with each other.

Hub-and-spoke topologies may be used, when sites from different customer VPNs needs access to shared services avoiding connectivity between the sites, e.g. for Internet access.

- Select the address family either IPv4 or IPv6 depending on the need of the customer..

- The values of QoS_profile dropdown list will depend on the address family. Select the default QoS profile of the service from the drop down list. This value will be passed onto all new sites in the VPN.

NOTE: QoS configuration is used to provide differentiated treatment of the traffic being exchanged between the provider network and the customer site.

VPN_SVP supports up to 8 classes of services (CoS). The VPN_SVP QoS components consist of Traffic classifiers and Profiles. The QoS profiles use the following naming convention

   <name>_p1.p2.p3.p4.p5.p6.p7.p8

where the p1,..,p8 are values from 0-100 that represents the percentage of the requested rate limit allocated each of up to 8 CoS. The sequences of CoS are as specified in the *EXP mappings* table in *SAVPN/Parameters*. E.g. with 5 CoS defined, the EXP mappings could be

Class Name	MPLS EXP	CE DSCP	Loss Priority	Queue
Best-Effort	1	8	high	bronze
Bronze	2	16	low	bronze
Silver	3	24	low	silver
Gold	4	32	high	gold
Platinum	5	40	low	gold

and the percentages would correspond to

- p1 ~ Best-Effort
- p2 ~ Bronze
- p3 ~ Silver
- p4 ~ Gold
- p5 ~ Platinum

and p6, p7and p8 will not be specified.

Hence, e.g. the profile *l3_simple_0.0.0.100.0* associates 100% of the customer traffic with the Gold CoS.

The QoS profiles implements rate limiting of ingress traffic and shaping of egress traffic on the Provider edge device.

Traffic classifiers determine which class data traffic belongs to. The techniques for this may be quite varied from simply stating that all traffic belongs to a specific class, to inspecting each and every packet and classify these individually (often implemented in router hardware).

VPN_SVP QoS supports configuration of the L3 classification to be based either on DSCP values or on IP addresses and TCP/UDP ports in the packet headers. The DSCP based classification allows you to specify a list of DSCP values (e.g. cs4,cs5), filter based classification supports the format: protocol://ip/mask:ports (e.g. tcp://10.1.1.1/32:1521 or udp://2001:db8:3c4d:15:0::2000/124:1456 in case of IPv6 based filters).

When traffic is forwarded into the MPLS core network, the CoS of the packet determines the EXP bit value the MPLS packet will be marked with. This value is selected from the *EXP mappings* table in *SAVPN/Parameters* view in the *Inventory GUI* and configured by VPN_SVP as part of service activation.

- Select the **VPN topology** type from the drop-down list. Your customer requests the *Hub and Spoke* topology.

- Select *Yes* for the **Managed CE Router** field from the drop-down list. The value will default to the sites which will be added to the VPN service later on; however it can be changed at the site level. Selecting *No* implies that the customer themselves manages the CE routers, and the provider will only supply configuration values (work-orders) required for the correct attachment of the CE routers.

- Select *Both* for the **Activation Scope** field. This value instructs Service Activator which edge devices have to be configured. The options include *PE_only, CE_only,* and *Both.* If the *PE_only* or *CE_only* value is selected then only the specified router is configured initially - it is still possible to continue and complete the activation process of the edge devices at a later point.

- In the field **Comments***,* you may add any service related notes, which will be forwarded to the Service Activator and will be visible to the network operator throughout the process of activation.

Service information	
layer3-VPN id	1003
VPN name	Sales
VPN topology	Full mesh
Site defaults	
address family	IPv4
QoS profile	l3_simple_0.0.0.100.0
managed CE routers	Yes
activation scope	Both
Comments	
	Add your comments here....

- Select the **Submit** button in the bottom right hand corner of the form to proceed. An xml message with the specified service parameters will be forwarded to Service Activator. You will be returned to the *Customer Services* form where you will find the newly defined service.

	Id ▲	Name	State	Type	Submit date	Action	Subservices	
	1003	Sales	Ok	layer3-VPN	15/04/2012	🔍✖️📝	layer3-Site	→

Existing services (1)   Page 1/1   Go to page 1   First   Previous   Next   Last

7-1-2 Add Layer 3 VPN Sites

Sites can now be added to the VPN service enabled for your customer in section 7-1-1 Enable Layer 3 VPN Service.

Follow these steps to add sites to the service:

- Navigate to the *Customer Services* form.

- Locate the newly created Layer3 VPN '*Sales'* in the *Existing Services* section

- Select the **Submit** button in the *Existing Services* with **Type** *'layer3-VPN'* and **Name** '*Sales'*, to requests a **Subservice** of type '*layer3-Site*' as indicated in the form.

- This brings up the *Create Services* form in which you must enter the layer3 site service related parameters.

- **layer3-Site id** is generated uniquely by the CRM portal system.

- Enter the name of the site in the **site name** field. In this example this is *Sales1.*

NOTE: The **site name** field may be entered in two ways: As an operator specified string in case of a new site is to be created or by selecting an existing site name from the drop-down list.

When a new site name is entered, the site will be automatically created as part of the request submitted to HPSA before the requested service then gets associated the site.

When an existing site is selected, the service will be added to the existing services, by using a service specific Vlan id on the access port that previously was chosen when the selected site was created. This is referred to as service multiplexing.

Not all combination of site services is permitted. Basically the existing site services, as well as the new service, must be port-vlan based.

The CRM Portal does not keep the detailed network information and may not in all cases be able to validate directly, if the selected service may be added using the specified Vlan id. As part of handling the request in HPSA when it is submitted, a service validation (or feasibility check) will be performed. If the check indicates that the new service may not be added to the existing site, a REUSE error will be raised.

- Select **region** value *Denmark* and the **location** value *Copenhagen* from the drop-down lists. These values indicate the region in the provider's network which covers this customer site. Locations limit the selection of PE routers that will be used to provide the service for this site.
- Select the 512Kbps value for the field **rate limit** from the drop-down list to specify customer site access rate.
- Select the silver **QoS Profile** value *l3_simple_0.0.100.0.0.* The service-level value was defaulted from the VPN set up to *l3_simple_0.0.0.100.0 for* the site; however it can be changed at the site level.
- Select the "Spoke" value for the *site* **connectivity type**. A site can either work as a spoke, as hub or as a meshed site. When the VPN topology is chosen as 'Hub and spoke' only values *Hub* or *Spoke* may be selected.
- Select *Yes* for the field **managed CE router***.* The service-level value was defaulted from the VPN set up to *No* for the site; however it can be changed at the site level.

NOTE: A **managed CE** router represents a CE router managed*,* and typically *owned* by the *provider*. Otherwise the CE router is managed and typically owned by the *customer* and the provider will not access nor configure the customer CE.

In both cases, the provider allocates important resources for the CE router to become attached to the provider's network and this information is needed when the CE router is being installed and pre-configured.

In the **managed CE** case, only the initial configuration allowing connectivity to the CE router is necessary to manually complete, the final activation is done by VPN_SVP.

- If the CE router is selected as managed, it is possible to select **CE Based QoS** as either *Disabled* or *Enabled.* When selected as *Enabled*, customer traffic will be classified and rate limited on the CE router. The traffic will be marked using DSCP values and on the PE router it will be re-classified and marked with corresponding EXP bits.
- Select *Both* in the field **activation scope**. The service-level value is defaulted to the site; however it can be changed at the site level.

NOTE: The **activation scope** controls the activation process of an L3 VPN site:

- *Both*
  The activation process is to include activation of both the PE and the CE routers. The request will be in **State** *In progress* until the PE and CE activation processes are both complete.

- *PE only*
  The process is to include activation of only the PE router. It will be optionally to follow up be selecting the sub-service: **Start CE activation** at a later time

- *CE only*
  The process is to include activation of only the CE router, at least initially. It is assumed, that the PE process will be selected later when the CE router is ready at the customer premises, by selecting the sub-service: **Start PE activation** or in case of a *managed CE* by selecting: **Start PE and CE activation.**

- Value for the field **address family** would be either IPv4 or IPv6. This value would be defaulted to the same chosen during the creation of VPN and the user would not be able to modify this value on the site level.

- Select a protocol value for the field **PE-CE routing**. Select e.g. RIP as the routing protocol between the PE and CE routers.

NOTE: VPN_SVP supports RIP, OSPF, eBGP and Static routes in the case of IPv4. For some of the supported routing protocols, additional information must be provided:

- OSPF: Customer area id must be supplied

- BGP: Customer ASN must be supplied

- Static routes: The specific static route entries must be provided

Static routes add by VPN_SVP will use the CE interface address as the 'next hop' address and metric 2.

When BGP is selected, an optional prefix-limit is supported.

In case of IPv6 VPN_SVP supports only OSPF, eBGP and Static routes.

NOTE: With BGP, the default prefix-limit set is 50. If the prefix-limit exceeds 1000, the value has to be approved by Admin/Manager. That is, these jobs are posted on the **confirm_eBGP_limit** queue for the admin operator interaction.

Active Jobs

| add_l3_site_pe(1) | confirm_eBGP_limit(1) | controller_queue(4) | Running Jobs | Scheduled Jobs |

| | | | Retrieve limited jobs | | | | Results 1 - |

VPN Info	Service Id	Workflow	Status	Start Time	Post Time	Step	Node Description
Customer:"Giga-tronics Inc. (22)" VPN:"LargeVPN(1075)" Site:"bigSite3(1083)"	1084	L3VPN_ReserveResource	Waiting	Nov 14, 2010 8:55:02 PM	Nov 14, 2010 9:00:04 PM	Confirm_eBGP_Limit	Confirm operator selected BGP Maximum Prefix value

Interact with the job in this queue to get the below form.

Interact with job: L3VPN_AddSite_PE

Job ID	Workflow	Start Date & Time	Post Date & Time	Step Name	Description	Status
108831	L3VPN_ReserveResource	Sun Nov 14 20:55:02 IST 2010	Sun Nov 14 21:00:04 IST 2010	Confirm_eBGP_Limit	Confirm operator selected BGP Maximum Prefix value	Running

Customer Name (Id) Giga-tronics Inc. (22)
VPN Name (Id) LargeVPN (1075)
Site Name (Id) bigSite3 (1083)

Maximum prefix: 5000

Confirm   Refuse

If admin Confirms the maximum prefix value, the job proceeds with the activation task. However, if the admin Refuses the maximum prefix value, the service creation operation Fails.

- Select a value for the field **PE-CE address pool** from the selection list, e.g. *PE-CE Default*. Address pools are created in the HPSA Inventory GUI SAVPN/Parameters view alternatively PE-CE Default IPv6 is created in the case of IPv6. The selection of the proper pool is important to avoid potential collision with the existing numbering scheme used at the customer's site. See [*ADM*] for more information about this issue.

- Select the **Submit** button to forward the site service request to Service Activator. You will be returned to the *Customer Services* form where you will find the new site entry added to the selected VPN service.

- HPSA communicates messages back to CRM portal about the progress of each activation requested which is indicated in the **State** column of the *Customer Services* view requests.

NOTE: The CRM portal keeps the **State** of a service updated in the *Customer services* view:

- *Request Sent* - Indicates that an activation request has just been issued and sent to Service Activator.

- *In Progress* - Indicates that the activation request is being process in Service Activator.

- *PE Waiting Operator* – Indicates that the activation request is waiting for the network operator interaction on HPSA and this State could persist for a considerable time.

- *OK* - Indicates that the activation has been completed.

- Failures will initially be handled by the network operator on HPSA using the ErrorHandler. Failed services will be in state *Temporary Failure* with n*o* **Actions** available until handled by the network operator. See chapter 10-2 for further information.

Service information	
VPN name (id)	Sales (1003)
layer3-Site id	1004
site name	Sales1
region	Denmark
location	Copenhagen
rate limit	512Kbps
QoS profile	l3_simple_0.0.100.0.0
Silver	l3_any 100 512Kbps
managed CE routers	Yes
CE based QoS	Disabled
activation scope	Both
address family	IPv4
PE-CE address pool	PE-CE Default
PE-CE routing	RIP
Scheduling information	
start time	Reset
end time	Reset
Comments	

NOTE: The layer3 Customer Site service is actually constructed from two services:

A layer3-Site service that represent the Customer site

A layer3-Attachment service that represent the interconnection between the customer site and the provider network.

When submitting a layer3 Site service request, both the Site and the Attachment requests are actually submitted.

The layer3-Site request completes without any need of network operator interaction.

The layer3-Attachment request needs the HPSA network operator to appoint the edge device and interface information, so this request enters 'Waiting Operator' state until this has been selected.

The view below illustrates how this is displayed in the CRM portal.

	Id △	Name	State	Type	Submit date	Action	Subservices	
	1003	Sales	Ok	layer3-VPN	15/04/2012	⟲✗☑	layer3-Site ▾	→
⊟	1004	Sales1	Ok	Site	16/04/2012	None		
	1005	-	PE CE Waiting Operator	layer3-Attachment	16/04/2012	None		

Existing services (3)   Page 1/1   Go to page 1   First Previous Next Last

The service delivery process continues with the activation task on the HPSA portal. See section 7-2 .

NOTE: VPN_SVP implements two generic processes for service activation. One process requires the network operator to supply extra information in HPSA and the other process is flow-through in nature and requires no interaction.

Addition of site services generally requires the network operator to select the point of attachment of the service, i.e. the edge device and the port/interface to be used for the service.

Modification and deletion of services generally requires no interaction as all necessary parameters are available in either the request or in the Inventory db.

7-2 Layer 3 VPN Site Service Delivery in HPSA

Service Activator enables network operators to monitor new jobs arriving from CRM Portal selecting the left pane *Jobs* view.

Requests for layer 3 VPN site services may, depending upon the *activation scope*, post two types of jobs for the network operator to interact with, i.e. PE router jobs and CE router jobs which corresponding to the selection of PE and CE edge resources.

● PE router jobs are posted on the **add_l3_site_pe** queue for network operator interaction

The CE router jobs are dependent upon the requested activation scope and upon whether they are managed (i.e. managed by the *provider*) or un-managed (i.e. managed by the *customer*).

● Un-managed CE router jobs generate only a work-order containing the parameters that the customer must know to set up their CE router correctly. No interaction by the network operator is required.

● The managed CE process may involve shipment, pre-configuration/installation at customer premises and final activation by VPN_SVP, refer section 5.4 of *ADM* for complete details on managed CE activation process. Managed CE router jobs requires:

- ○ The interaction by a network operator to supply the details of the CE router and its initial configuration parameters that must be completed before connectivity to the provider network is possible. These jobs are posted on the setup_ce queue. Alternatively the CE routers can be pre-populated in the inventory either through HPSA Inventory UI or through the import utility.

- ○ When submitting the **setup_ce** form, the process generates a work-order that contains the necessary parameters for the personnel, responsible for shipping/initial setup and attaching the CE router to the provider's network, to complete their tasks. After this step, now the decision on when the CE router should be activated needs to be done by northbound system operator like CRM operator.

- ○ Upon the initiation of 'Start CE activation' from the northbound system / CRM, the final configuration of the CE router may proceed and will be completed automatically by HPSA.

- ○ If the CRM operator did submit the request with **activation scope** *CE_only,* the process completes on HPSA after the interaction with **setup_ce** form , and control is returned back to CRM operator. The CRM operator may now proceed with the final activation of the PE router (and CE router) be selecting the sub-service: *Start PE and CE activation* (see section 7-1-2 above).

- ○ It is possibly to indicate in the **setup_ce** form, that the CE router is **not present,** i.e. the CE router is not yet installed and connected to the provider's network at the customer premises. In this case only the work-order is generated and the control is passed to the CRM to start the CE activation, when the router is ready. The final configuration of the CE router normally done automatically by HPSA is skipped. It is assumed, that the CE router will be configured in some other way outside of VPN_SVP.

The selection and necessary interactions with these PE and CE related jobs may be performed by separate groups of operators depending upon the desired procedures of the provider.

7-2-1 Activate PE Router for Layer 3 VPN Site Service

All jobs related to the selection of provider edge device and the port/interface are posted on the **add_l3_site_pe** queue. Follow these steps to activate your edge routers for the L3 service requested in 7-1-2 Add Layer3 VPN Sites:

- Log in to Service Activator.

- Select *Jobs* from the *Work Area* menu in the left navigation pane. This will open the *Active Jobs* form.

- Go to the **add_l3_site_pe** tab to locate the jobs to interact with and right click on the selected job. This will open an additional pop-up menu.

- Select **Interact with Job** from the additional menu.

Active Jobs

add_l3_site_pe(1)	controller_queue(1)	Running Jobs	Scheduled Jobs

| | | Retrieve limited jobs | | | | Results 1 - 1 |

VPN Info	Service Id	Workflow	Status	Start Time	Post Time	Step	Node Description
Customer:"Baldor Electric Company (22)" VPN:"Sales (1054)" Site:"Sales1 (1055)"	1056	L3VPN_ReserveResource	Waiting	Interact with Job Stop Job		Select_PE_Router_And_If	Select the PE router and the interface on the selected PE router.

- This provides the interface to the network operator for the selection of the provider edge device and the access port to where the service is to be attached.

- The form provides identifying information including the optional CRM operator comment. The information includes the *Location* selected in CRM portal and which is used to limit the selection list of available edge devices in the **Select Router** list.

- The **Select Router** list of available edge devices will include access devices if access networks are defined within that location (as described in section3-7). Hence, it is possible to select direct attachment on PE routers (N-PEs) or attachments via access networks by selecting access devices (U-PEs or Aggregation switches)

- Select the desired edge device among the ones available for this location presented in **Select Router** list.

- The selected router may have E1 or STM1 controllers defined in which case a **Create Interface** button will be available in the above form. This may be used to create a serial interface associated an E1 channel-group (see section 8-4 Channelized Interfaces for more information) 'just-in-time' for service activation.

- When the edge device has been selected, its available interfaces will be presented in the **Select Interface** list from where the desired interface may be selected.

NOTE: In the case you desire to use an Ethernet interfaces type, note that if the requested *rate limit* is less than 2Mb, interfaces with bandwidth higher than 10Mb are not selectable.

- Select the encapsulation of the PE-CE attachment circuit from **Select Encapsulation** list. For Serial interfaces, encapsulation may be set to *HDLC, PPP* or *FrameRelay*. For Ethernet interface encapsulation *none* or *dot1Q* may be selected.

NOTE: The available encapsulations depend on the type of the interfaces.

Serial interfaces support the following encapsulations: *HDLC, PPP* or *FrameRelay*.

Ethernet interfaces supports the following encapsulations: *none* or *Ethernet-dot1Q*

In the case of *FrameRelay* encapsulation the **DLCI** value, and in the case of Ethernet-dot1Q encapsulation the **Vlan Id** value, may be specified as either **Customer Provided** or **Provider Managed.**

Customer Provided allows the value to be selected among the values in the **DLCI**/**Vlan ID** selection list.

Provider Managed specifies that automatic allocation of an available value will be made by VPN_SVP.

The allowed ranges for the Vlan ID/DLCI values are constrained by the defined global scheme in *Inventory GUI→ SAVPN/Parameters→Parameters→SP parameters→Vlan ranges/DLCI ranges* object. (See also the Note in section 0).

In the case of *FrameRelay* encapsulation, it will also be possible to specific the **LMI type** as *ansi*, *cisco* or *q933a* and the **INTF type** as *dte or dce*

If the encapsulation of an interface already has been specified by some earlier service requests, it is protected and it will not be possible to change it.

When the access port is selected on an access switch/aggregation switch, and the selected access network is attached to multiple N-PEs, it is optional to enable VRRP. This creates a single virtual router out of the multiple N-PEs to provide resilience towards router failure. The VRRP feature allows the selection of the Master Router among the available N-PEs, as shown in the figure below

- Select the **VRRP** checkbox, in case redundancy option is required. When VRRP checkbox is selected, the other VRRP fields are displayed.

- Select the **Master** PE from the dropdown list.

- Select the **VRRP Group ID** from the dropdown list. This is the group to which both the Master and the backup router will belong.

- Select the **Submit** button. HPSA will now have all the necessary parameters available and will continue with the activation and configuration of the selected port on the selected device(s).

NOTE: When an access port/aggregation switch port has been selected as the attachment point, HPSA will configure the access port and the trunk ports and in the access topology in addition to the MPLS service configuration on the N-PE sub-interface.

In case any error occurs during the configuration of the device, an error message will be posted to the HPSA Messages→**Errors** messages queue and the job will be posted on the failed-jobs queue for further analysis and diagnostics. See chapter 10 for further information on Error Control.

In case of a hopefully temporary, connectivity failure between VPN_SVP (the NOC) and the selected device, the service request is automatically rescheduled by the Delayed activation handler. See chapter 10 for further information.

In the normal case of a successful activation, a response will be send back to the CRM portal and the state will be updated accordingly.

7-2-2 Activate CE Router for Layer 3 VPN Site Service

As described above, the CE router activation process is dependent upon the requested activation scope and upon whether the CE router is managed (i.e. managed by the provider) or un-managed (i.e. managed by the customer). Refer section 5.4 of *ADM* for complete details on managed CE activation process.

7-2-2-1 Un-managed CE Router Set-up

If the CE router is un-managed (i.e. the managed CE router attribute is *No*) it is assumed that the customer manages the device, and it is the customers own responsibility to configure the CE router's PE facing interface with the correct IP address, network mask and routing protocol. VPN_SVP will reserve the IP addresses for the PE-CE link which the provider may supply to the customer in the form of a work-order.

HPSA will normally generate a work-order for l3 service requests, but if the CRM **activation scope** was selected as *PE only* the work-order will not be generated until the CRM operator optionally continues the process by selecting the sub-service: *Start CE activation.*

NOTE: When activation scope *CE only* has been selected, the allocation of IP addresses need to assume that the CE eventually could become attached to the provider network via an access network. To accommodate the possibility of multiple aggregation switches and N-PEs, an IP network address with mask of /29 will be allocated from the specified address pool.

The provider may submit the work-order information to the customer, either manually or by automated distribution to the customers' contact person's email address (this may be achieved by following the configuration as described in section 8-5 below). The customer must then configure the CE router accordingly. [relook – at what's said in the section 8-5].

7-2-2-2 Un-managed CE Router Work-order

Service Activator will generate a work-order for the CE with the necessary configuration information for the customer's configuration engineer to complete the configuration of the CE router. The work-order is saved in the database and may be accessed via the HPSA left navigation pane *Tools*→*Work-orders* menu.
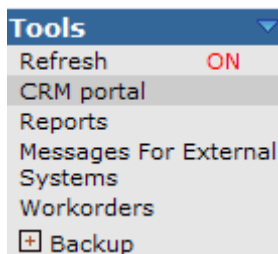
The work-orders are listed and their names correspond to the service type and service id.

Work-orders

Service Id ▼	WOName	Date
1210	Workorder_L3VPN_SetupSite_CE_1210.xml	2008-08-05 16:45:56.0
1207	Workorder_L3VPN_SetupSite_CE_1207.xml	2008-08-05 16:10:35.0
1205	Workorder_L3VPN_SetupSite_CE_1205.xml	2008-08-05 15:40:00.0
1181	Workorder_L3VPN_SetupSite_CE_1181.xml	2008-08-04 15:26:23.0
1168	Workorder_L2VPWS_SetupSite_CE_843_1160.xml	2008-08-01 14:30:25.0
1167	Workorder_L2VPWS_SetupSite_CE_834_1160.xml	2008-08-01 14:30:24.0
1143	Workorder_L3VPN_SetupSite_CE_1143.xml	2008-07-30 16:33:03.0

Reset   <<   < Prev   1 - 7 / 14   Next >   >>   Go

So, e.g. for the job with service id 1205, the CE work-order is named:

`Workorder_L3VPN_SetupSite_CE_1205.xml`

Click (left-click) the entry to view the content of the work-order. The content of the work-order may look as shown below. The Work-order view allows you to **save** the work-order as file or to **print** the work-order. You may use this for manually distribution of the work-order to the customer.

VPN_SVP also supports automated distribution of un-managed CE work-orders to the customers' contact person's email address. This may be achieved by following the configuration as described in section 8-5 below.

Workorder_L3VPN_SetupSite_CE_1205.xml

INFORMATION FOR SETTING UP CE ROUTER AT CUSTOMER SITE

Date: 2008.08.05 15:39:59

Order parameters:

Customer Name	Giga-tronics Inc.
Contact Person	John Schmidt: 328-4650
Region	Denmark
Location	Copenhagen
L3 VPN Name	bigVPN
L3 VPN Id	1000
L3 Site Name	bigSite6
L3 Site Service Id	1204
L3 Attachment Id	1205
Comment	

Interface towards provider:

IP address	172.17.0.42
IP network	172.17.0.40
Netmask	255.255.255.252
Hostmask	0.0.0.3

Provider Interface details:

Interface Name	Ethernet1/0
VLAN Id	2005
Encapsulation	dot1Q

Routing infomation:

Routing Protocol	RIP

Save   Print

7-2-2-3   Managed CE Router Setup

The main steps in the process of activating a managed CE router are:

- Creation of CE in VPN_SVP inventory either using the UI or XML Import utility.
- Allocation and assignment of resources in VPN_SVP to be used for the requested service associated with the generation and distribution of the initial configuration (set up) of CE router in the form of a work-order
- Installation of the CE router at the customer premises and manual configuration of the CE router according to work-order – manual step.
- Attaching the CE router to the Provider network – manual step.
- Final configuration of the CE router.

The final configuration is done automatically by VPN_SVP when the CE router is present (i.e. installed and attached) but only after the PE interface has been successfully provisioned.

Assume that customer *Baldor Electric Company* has requested the CE Router to be managed by the provider.

- The CE network operator is notified through the **setup_ce** jobs queue that a new job has been submitted.

Active Jobs

VPN Info	Service Id	Workflow	Status	Start Time	Post Time	Step	Node Description
Customer:"Baldor Electric Company (22)" VPN:"Sales (1054)" Site:"Sales1 (1055)"	1056	L3VPN_SetupSiteAttachment_CE	Waiting	Interact with Job / Stop Job		_CE_information	Request additional information for CE router

controller_queue(0) setup_ce(1) Running Jobs Scheduled Jobs

Retrieve limited jobs   Results 1 - 1

- The network operator interacts with the job on the **setup_ce** queue which provides a form to fill in the information about the new CE router.

Interact with job: L3VPN_SetupSite_CE

Job ID	Workflow	Start Date & Time	Post Date & Time	Step Name	Description	Status
108529	L3VPN_SetupSiteAttachment_CE	Sun Nov 14 16:23:13 IST 2010	Sun Nov 14 16:23:15 IST 2010	Get_CE_information	Request additional information for CE router	Running

Customer name   Giga-tronics Inc.

VPN Name   Sales

Site Name   Site1

Site Service ID   1054

Attachment Service Id   1055

Comments

Name of CE router   GigaTronics_CE

Management protocol   telnet

Is username authentication enabled on router? ○ Yes ⊙ No

Router password   ••••••••

Enable password   ••••••••

Vendor of router   Cisco

OS Version   Cisco-12.2

Model of CE router   C2600

Serial Number   S/N 345d45d22

Is the CE-router present?   ○ Yes ⊙ No

Interface type   Ethernet

Interface name   FastEthernet0/1

RO Community   public

RW Community   private

Submit   Clear

- When the CE set-up configuration form is completed, use the **submit** button to save the data.

The HPSA Equipment Inventory will now be populated with a new CE router object in the requested region (e.g. *Denmark*) containing the service relevant information. Also, the work-order containing pertinent information for initial set-up of the CE router is generated and saved in the database. Alternatively CE router can also be pre-populated either using HPSA Inventory UI or using XML import utility provided by VPN_SVP.

Follow these steps to locate the work-order containing the relevant information for configuring the CE router:

● Log in to Service Activator.

● Select *Workorders* from the *Tools* menu.

● Locate the work order by the time-stamp or by the attachment service id of the request (i.e. 1046) and select it

Work-orders

Service Id ▼	WOName	Date
1056	Workorder_L3VPN_SetupSite_CE_1056.xml	2009-10-16 16:57:37.0
1045	Workorder_L2VPWS_SetupSite_CE__1048.xml	2009-10-16 16:19:32.0
1043	Workorder_L2VPWS_SetupSite_CE__1047.xml	2009-10-16 16:19:31.0
1023	Workorder_L2VPN_SetupSite_CE_1023.xml	2009-10-16 15:30:12.0

Reset   <<   < Prev   1 - 4 / 4   Next >   >>   Go

● The work-order form like the following will be displayed

Workorder_L3VPN_SetupSite_CE_1056.xml

INFORMATION FOR SETTING UP CE ROUTER AT CUSTOMER SITE

Date: 2009.10.16 16:57:37

Order parameters:

Customer Name	Baldor Electric Company
Contact Person	John Doe: +11 223344
Region	Denmark
Location	Copenhagen
L3 VPN Name	Sales
L3 VPN Id	1054
L3 Site Name	Sales1
L3 Site Service Id	1055
L3 Attachment Id	1056
Comment	

CE Router box:

Name	BaldorSales1
Vendor	Cisco
Type	C2600
OS version	Cisco-12.2

Configuration parameters of CE router:

Password	password
Enable password	password

Loopback interface:

IP address	10.20.30.0
Netmask	255.255.255.255

Interface towards provider:

Interface Name	FastEthernet 0/1
IP address	172.17.0.10
IP network	172.17.0.8
Netmask	255.255.255.252
Hostmask	0.0.0.3
RO Community	public
RW Community	private

Provider Interface details:

Interface Name	Ethernet1/0
VLAN Id	3001
Encapsulation	dot1Q

Routing infomation:

Routing Protocol	RIP

Save | Print

The manual configuration and installation of the CE router at the Customer's premises may be done by external operators after shipment of the CE router or it may be done internally before shipment depending upon the provider's procedures.

The router passwords must be set, the PE facing interface configured with the IP address and the default static route must be set to enable HPSA to connect to the CE router when its configuration is to be completed.

NOTE: In the case of the above work-order, the interface on the PE router was selected as Ethernet Dot1Q encapsulated with a Vlan id of 3001 associated and that the provider facing interfaces on the newly created CE router was selected as FastEthernet 0/1. It is no requirement that the two interfaces are of identical type and encapsulation although this probably would be the most common case.

VPN_SVP also supports automated distribution of un-managed CE work-orders to the customers' contact person's email address. This may be achieved by following the configuration as described in section 8-5 below.

● When the CE router set-up has been completed the act of performing CE activation is delegated to a north bound system like CRM.

	Id ▲	Name	State	Type	Submit date	Action	Subservices	
	1003	Sales	Ok	layer3-VPN	15/04/2012	⚙✗✎	layer3-Site ▼	→
−	1004	Sales1	Ok	Site	16/04/2012	⚙		
	1005	-	PE CE Ok	layer3-Attachment	16/04/2012	⚙✗✎	Start CE activation	→

Existing services (3) Page 1/1 Go to page 1 First Previous Next Last

● Select the Submit button to forward the 'Start CE Activation' request to Service Activator. Once the activation is done the CRM state would move to "Ok".

VPN_SVP will now proceed with the activation process and complete the final activation of the CE router automatically. This includes setting up the loopback address (management) address of the CE router and configuring the requested routing protocol on the requested interface.

VPN_SVP supports a remote CE provisioning process, where work-orders are distributed automatically to e.g. 3rd-party technician's email addresses, configurable per Region and Location.

NOTE: In case of an *un-managed CE* (**managed CE router** is selected as '*No)'*, no activation towards the CE router will ever be attempted. Even if you select sub-service *'Start CE activation'* only a work-order will be generated.

In case of a *managed CE*, the configuration of the CE router will only be done. It's now the responsibility of the north-bound system operator to 'Start CE activation' after making sure that, that the CE is actually present and preconfigured as prescribed. A work-order will also be generated.

If the CE is specified as *Not present* in the setup_ce form, final activation of the CE will be skipped but a work-order will be generated.

7-3   View Layer 3 VPN Service

7-3-1   View Service in HPSA Inventory

Once a new service has been successfully delivered, it is possible to locate the service in the HPSA inventory view. To view the service for Layer 3 VPN sites:

- Log in to Service Activator.

- Navigate to the *Inventory* and select the *SAVPN/Services* view.

- Expand the *Customers* branch, locate and expand the *Baldor Electric Company* branch.

- Expand the *Layer 3 VPN Sites* branch to confirm that the new site has been added.

- Select the newly created Layer 3 site *Sales1* as created above in section 7-1-2

The *SAVPN/Services* hierarchy allows you to drill further into more information about the created site services to see the **SiteAttachment** or to see e.g. the **VRF** details.

The **SiteAttachment** (or Flowdomain) object represents the shared connectivity object associated a site service. This contains e.g. the Vlan id associated with the attachment, the IPNet, generally the attributes that are shared among the flowpoints. Multiple flowpoints may be associated the same attachment, each representing a termination point in the flowdomain, e.g. when multiple N-PEs are associated an access network.

You may also want to view the resource reservations related to your created L3 VPN site service

- In the *Inventory*, select the *SAVPN/Equipment* view.

- Expand region *Denmark* branch and locate your network.

- Expand the network branch and **PE routers** branch to locate the router selected for the service created in section 7-2-1 above (e.g. C3600-1).

- Expand the selected router branch to view **Interfaces** and expand the **Interfaces** branch.

- The interfaces used for services are reserved in the Inventory and this is marked by the **r** next to the interface icon. In the case that sub-interfaces are used for the services, these are created under their parent interfaces and these become marked with the branch expand symbol.

- Expand the parent interface *ethernet1/1* of C3600-1 router in the network *Copenhagen,* and select the reserved (**r**) sub-interface **ethernet1/1.3001** that represents the Vlan 3001 associated sub-interface that was selected in section 7-2-1 above.

The *SAVPN/Equipment* hierarchy allows you to drill into the interface related details such as bandwidth, encapsulation, Vlan ids, etc.

NOTE: The association of Ethernet Vlan ids and/or frame-relay DLCI values is modeled by sub-interfaces created under their parent interfaces and named according to the Vlan/DLCI value and displayed this way.

For L3 service termination points this is quite closely related to how Ethernet interfaces are represented in most vendor equipment, whereas for Frame-relay the actual device representation may differ somewhat more from this model.

The *SAVPN/Equipment* hierarchy ends at the **Flowpoint** details on the selected (sub-)interface.

● Expand e.g. the sub-interfaces branch associated **ethernet1/1.3001** and select the **Flowpoint**.

The **Flowpoint** details allow you to link to the associated service that is using the selected (sub-)interface by inspecting the **AttachmentId** attribute (e.g. 1046). This id identifies the SiteAttachement object that is located in the *SAVPN/Services* view hierarchy as describe above.

7-4 Modify Layer 3 VPN Service from CRM Portal

Existing Layer 3 VPN Services are modified from CRM Portal.

7-4-1 Modify Layer 3 VPN Service

● Log in to CRM Portal.

● Find your customer e.g. *Baldor Electric Company* and open the *Customer Services* form. (See also 4-3 Search for Customer Records for navigation instructions).

● In the *Existing* Services area of the *Customer Services* form, select the *Modify Service* icon next to the service you intend to modify. This will open the *Modify* form.

Several parameters of L3 Services are modifiable.

For the L3 VPN service you may modify the following parameters:

● *Topology* – Allows you to change the default connectivity type of your L3 VPN Sites. Select 'Hub and spoke' to allow additions of Hub or Spoke sites. Select 'Full mesh' to allow addition of fully meshed sites.

● *Multicast* – Allows you to enable multicast service for your L3 VPN Sites. This is due to vendor restriction only supported for Full mesh VPNs. You may specify *sparse* or *sparse-dense* mode.

For L3 VPN Site Attachment service you may modify the following parameters:

- *Connectivity type* – Allows you to change the site between *Hub* or *Spoke* for a site in a VPN with topology Hub and spoke

- *Join/Leave VPN* – Allows you to *Join* a site into multiple VPNs, e.g. intranet, extranet and/or internet type VPNs. Likewise you may *Leave* some of the VPNs you have previously Joined.

- *Multicast* – Allows you to enable multicast VPN on a per site basis. The first site being enabled will be forced as RP if VPN is in *sparse* mode

- *Rate limit* – Allows you to control the rate limit associated each individual attachment circuit

- *QoS* – Allows you to control the rate limit and QoS profile associated each individual attachment circuit

- *Add/Remove static routes* – Allows you to associate static routes to each individual attachment circuit.

Finally, you may add a protection attachment to an existing L3 VPN Site, when the BGP protocol has been configured as the PE-CE routing protocol.

7-4-2 Modify Rate Limit of Layer 3 VPN Site Attachment Service

A L3 VPN Site may be connected to the provider network via multiple attachment circuits and each individual attachment circuit may have its *Rate limit* modified. Below is illustrated how to modify the *Rate limit* associated a Site attachment circuit:

- To modify a customer site access rate, select in the *Existing* Services area of the *Customer Services* form, the *Modify Service* icon next to the service type *layer3-Attachment* of the Site attachment you intend to modify.

- Select *Rate limit* from the drop-down list for the field *parameter to modify*.
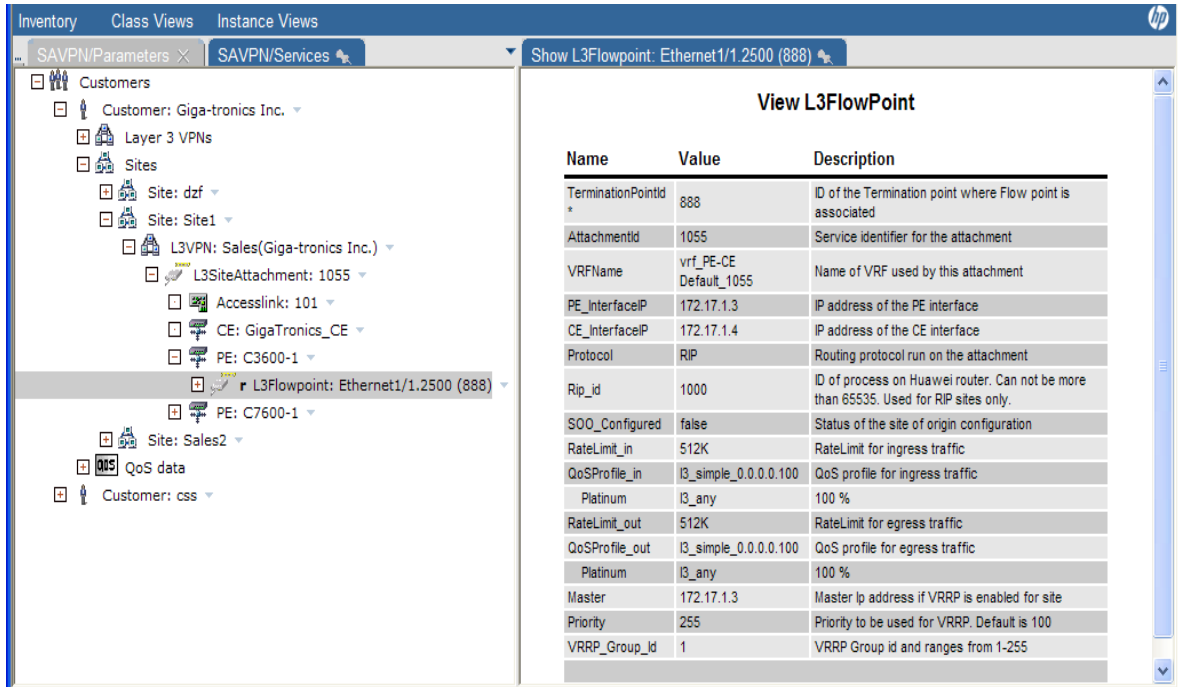
- Select a new access rate for the site attachment circuit from the drop-down list and choose the **Submit** button.

Your request to modify the service will be forwarded to Service Activator. The service request will start a workflow in Service Activator which will manage the activation of the router and will change the router configuration for the given service without any network operator interactions needed.

To view the result of site modification in Service Activator:

- Log in to Service Activator.

- Navigate to the *Inventory GUI window*.

- Select the *SAVPN/Services* view and expand the *Customers* branch.

- Locate your customer and expand its branch.

- Expand the *Layer 3 VPN Sites* branch.
- Expand the site which contains the attachment which was modified.
- Expand the 🖉 **SiteAttachment** branch corresponding to the modified attachment circuit
- Expand the 🖥 **PE** router branch and select the **L3Flowpoint** where the requested **RateLimit**'s may be observed

7-4-3 Join/Leave of Layer 3 VPN Site Attachment Service

The Join operation allows you to build more complicated connectivity structures among the sites in different VPNs. The customer may have a need that some sites, although in different VPNs, still must be able to communicate (intranet) or the customer may have the need for some sites to communicate with sites in another customer's VPN (extranet). You may also have the need to provide some services (e.g. Internet access) via provider owned VPNs that some customer sites then get joined into (e.g. Internet access).

The Leave operation allows you to perform to opposite of Join, i.e. withdraw a site from a specific VPN.

NOTE: When a L3 VPN site is created, it is owned by the customer that owns the VPN. It is not possible to leave this ownership relation. Hence, although it is possible to migrate among the VPNs owned by one and the same customer, it is not possible to completely leave all the customer's VPNs. Also, when a site is joined into another customer's VPN, it is visible in CRM portal in this VPN, but it is not modifiable from that services view.

- Log in to CRM Portal.
- Find your customer e.g. *Baldor Electric Company* and open the *Customer Services* form. (See also 4-3 Search for Customer Records for navigation instructions).
- In the *Existing* Services area of the *Customer Services* form, select the *Modify Service* 📝 icon next to the L3 VPN Site Attachment service you intend to modify. This will open the *Modify* form.
- Select *Join VPN* from the drop-down list for the field *parameter to modify*.

- Select e.g. *join extranet* for action. A customer selection drop-down list will appear which consists of customers having L3VPN services.

Service information		
layer3-AttachmentId	Sales1layer3-Attachment (1005)	
parameter to modify	Join VPN ▼	
action	join extranet ▼	
customer	Giga-tronics Inc ▼	
join to	Research ▼	
topology	Hub-and-Spoke	
connectivity	spoke ▼	
		➔

- Select **join extranet** option
- Find and select the extranet **customer** e.g. *Giga-tronics Inc.* and the **join to** drop-down list will consist of the L3VPN services of customer *Giga-tronics.*
- Select e.g. the L3 VPN Research (which is assumed to have been created earlier). Note that when the destination (join to) VPN is of topology Hub and Spoke, it must be specified if the site is to be joined with connectivity type Hub or Spoke into that VPN. When destination topology is Full-Mesh, the connectivity type can only be Mesh.

To view the result of the Join L3 VPN site modification in CRM

- Log in to CRM Portal.
- Find your customer e.g. *Baldor Electric Company* and open the *Customer Services* form. (See also 4-3 Search for Customer Records for navigation instructions).
- In the *Existing services* area of the *Customer Services* form, locate the site attachment service that was joined above. Note that the normal modify operation, etc are still available for this site.
- Select and click the service id link. This will open the *Service* view of this particular site service. Note the fields named *Related services* list the VPNs this site is a member of, including the newly joined *Finance (Giga-tronics Inc.)* where *Giga-tronics Inc.* is a link to the Customer Services view of *Giga-tronics Inc.*

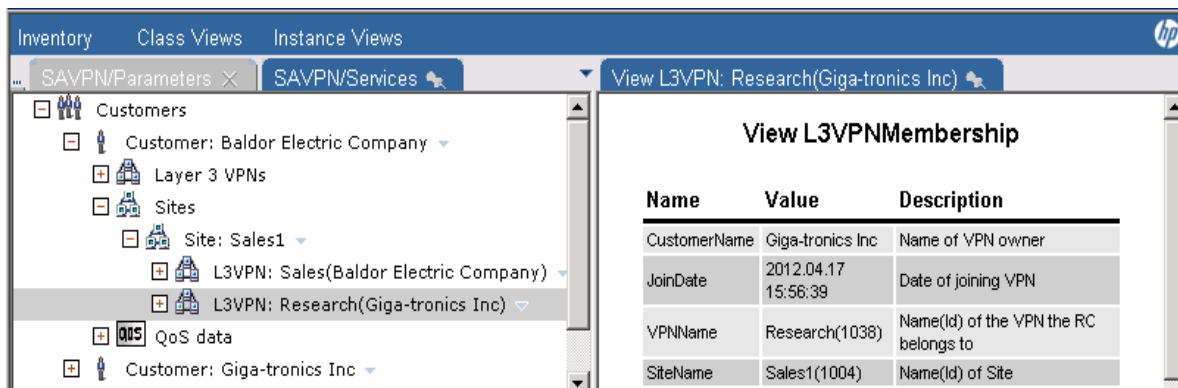| Related services	
Service	**Attribute**
Sales(Baldor Electric Company)	mesh
Research(Giga-tronics Inc)	spoke
	✗

- Select and click the *Giga-tronics Inc.* link. This will open *Customer Services* form of *Giga-tronics Inc.*

Existing services (3)		Page 1/1		Go to page 1		First	Previous	Next	Last

	Id ▲	Name	State	Type	Submit date	Action	Subservices	
	1038	Research	Ok	layer3-VPN	17/04/2012	🔒✗📝	layer3-Site ▾	→
⊟	1039	Research_1	Ok	Site	17/04/2012	🔒		
	1040	-	Ok	layer3-Attachment	17/04/2012	🔒✗📝		
	1004	Sales1 (Baldor Electric Company)	Ok	Site	16/04/2012			

NOTE: The joined site is listed with a link named *Baldor Electric Company* and that it is not possible to manage the site from this view. Because the site is owned by *Baldor Electric Company* and not by *Giga-tronics Inc.*

To view the result of the Join L3 VPN site modification in Service Activator

- Log in to Service Activator.
- Navigate to the *Inventory Tree* GUI.
- Select the *SAVPN/Services* view and expand the *Customers* branch.
- Locate your customer and expand its branch.
- Expand the *Layer 3 VPN Sites* branch.
- Expand the site which was modified above.
- Select the *VPN* that the site was joined into, to view the VPN membership parameters. In this example, it was *VPN: Research* owned by *Giga-Tronics Inc.*

7-4-4 Modify Multicast of Layer 3 VPN Service

The VPN_SVP supports configuration of Layer 3 Multicast VPNs. The multicast technology is PIM based and the sparse and sparse-dense modes are supported.

Before you may configure the sites to become members of a multicast VPN, these must be members of an ordinary Full mesh VPN.

NOTE: Multicast services can not be created on a Hub-and-Spoke VPN. It is supported only for Full Mesh VPNs.

- Log in to CRM Portal.
- Find your customer e.g. *Baldor Electric Company* and open the *Customer Services* form. (See also 4-3 Search for Customer Records for navigation instructions).

- In the *Existing* Services area of the *Customer Services* form, select the *Modify Service* ✎ icon next to the L3 VPN service you intend to modify. This will open the *Modify* form.

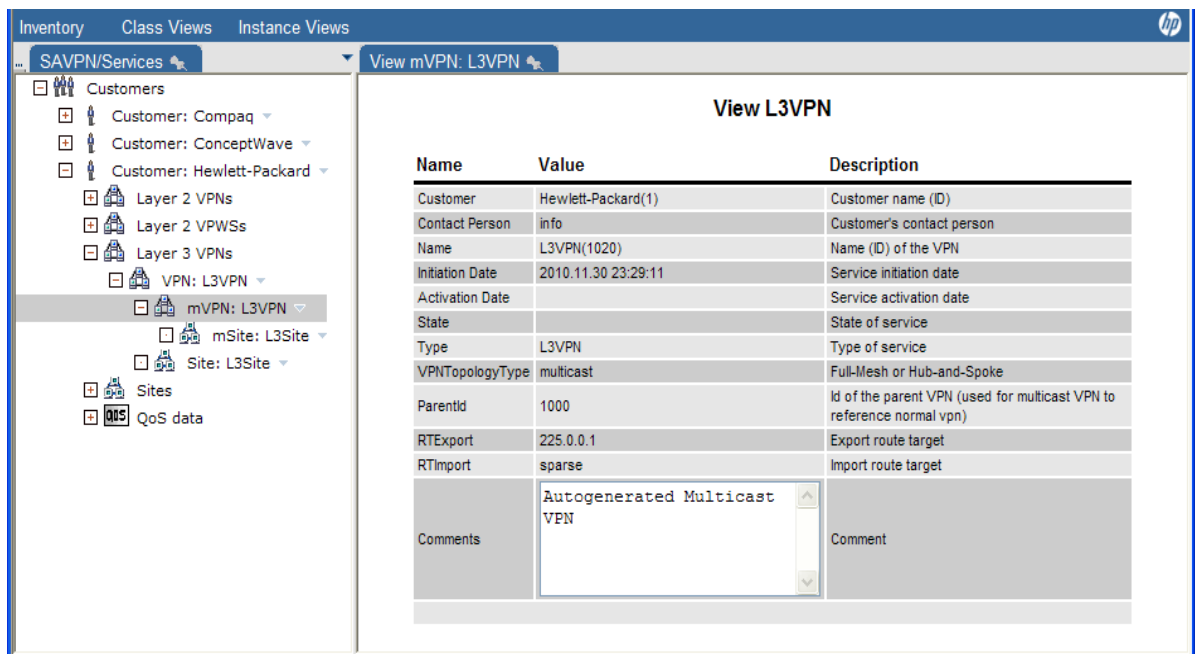- Select *Multicast* from the drop-down list for the field *parameter to modify*.

- Select *enabled* for Multicast VPN

- Select e.g. *sparse* mode from the drop-down list for Multicast VPN mode and choose the **Submit** ➡ button.

Your request to modify service will be forwarded to Service Activator. The service request will start a workflow in Service Activator which creates the multicast VPN objects and allocates a shared MDT Default multicast group address. No equipment configuration takes place due to this request.

To view the result of L3 VPN multicast modification in Service Activator, you should:

- Log in to Service Activator.

- Navigate to the *Inventory Tree* window and

- Select the *Services* view and expand the *Customers* branch.

- Locate your customer and expand its branch, and expand the *Layer 3 VPNs* branch.

- Notice that an mVPN has been auto-generated. Select the *mVPN* to display the multicast VPN specific parameters

- Notice that an MDT default group address (225.0.0.1) has been allocated from the MDT Default IP address pool and associated the mVPN. This is the unique multicast group address shared by all sites participating in this mVPN.

7-4-5 Modify Multicast of Layer 3 VPN Site Attachment Service

When multicast has been enabled for a fully meshed Layer 3 VPN you may enable multicast for the individual sites attachments so these become members of the multicast VPN.

- Log in to CRM Portal.

- Find your customer e.g. *Baldor Electric Company* and open the *Customer Services* form. (See also 4-3 Search for Customer Records for navigation instructions).

- In the *Existing* Services area of the *Customer Services* form, select the *Modify Service* 📝 icon next to the L3 VPN Site Attachment service you intend to modify. Please note, that multicast is only supported for Full mesh VPNs. This will open the *Modify* form.

- Select *Multicast* from the drop-down list for the field *parameter to modify*.

Service information		
layer3-AttachmentId	Sales1layer3-Attachment (1005)	
parameter to modify	Multicast ▾	
multicast VPN id	1044	
multicast site	enabled ▾	
RP point?	no ▾	
QoS Class	Gold ▾	
rate limit	512K ▾	
		➡

- In the form, select *enabled* to join the site attachment into the multicast VPN.

- It must be specified, in sparse mode, if the site is to be a RP (Rendezvous Point).

NOTE: When a L3 Multicast VPN is mode sparse, one or more sites may be specified as RPs. The RPs will automatically be associated a loopback interface and an IP address from the *Multicast loopback* pool.

Please note, that the first site of a L3 VPN being multicast enabled will be forced as a RP. Subsequent sites may optionally be selected as RP.

- The data traffic class you want the multicast traffic to be associated, is selected from the *QoS Class* drop-down list

- The Rate limit of the multicast traffic on this site is selected from the *rate limit* drop-down list..

NOTE: "Multicast bandwidth policy" flag under the inventory
SAVPN/Parameters→Parameters→Layer 3 parameters→Multicast Bandwidth Policy determines the bandwidth allocated to the multicast enabled site.
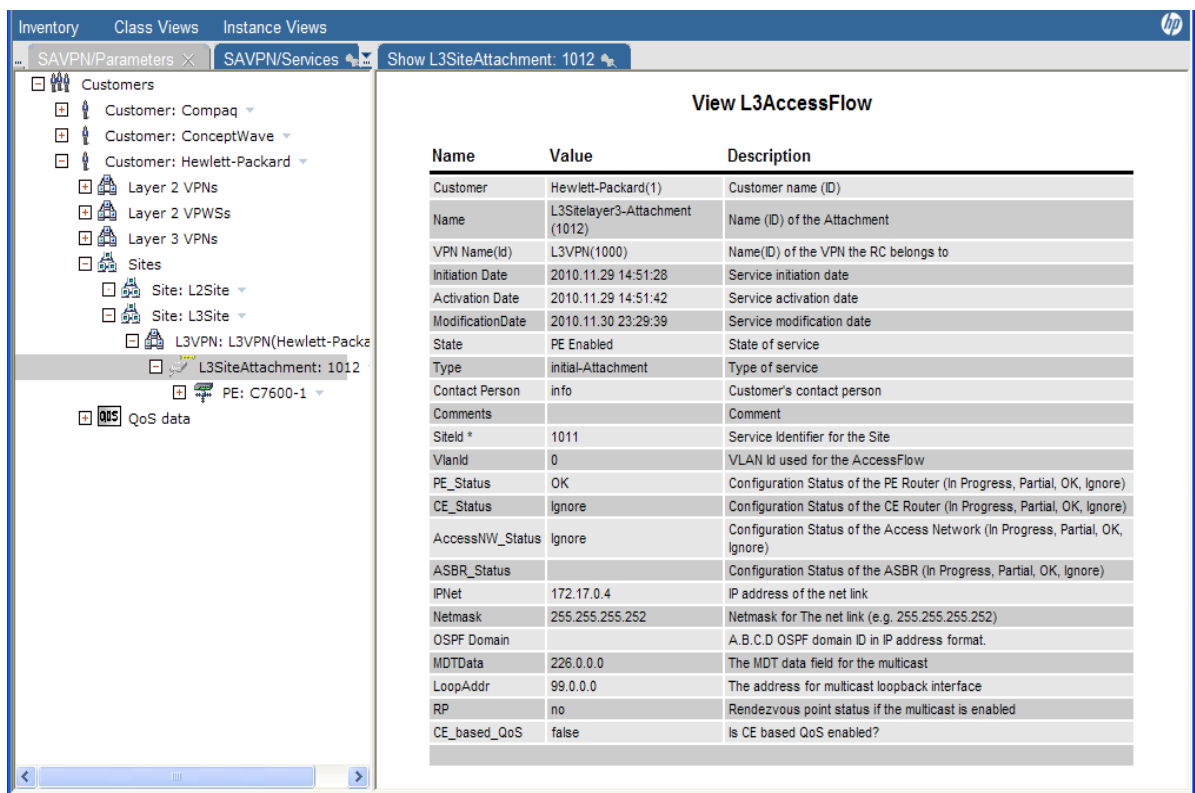
If this flag is false (default), the rate limit applied to the multicast service can not exceed the rate limit associated with the L3 VPN site.

If this flag is true, the rate limit applied to the multicast service may exceed the rate limit associated with the L3 VPN site.

- Select the **Submit** ➡ button. Service Activator will proceed with the activation and configure the multicast service.

To view the result of L3 VPN Site Attachment multicast modification in Service Activator:

- Log in to Service Activator.
- Navigate to the *Inventory Tree* window.
- Select the *Services* view and expand the *Customers* branch.
- Locate your customer and expand its branch.
- Expand the *Layer 3 VPN Sites* branch.
- Expand the site which was modified above.
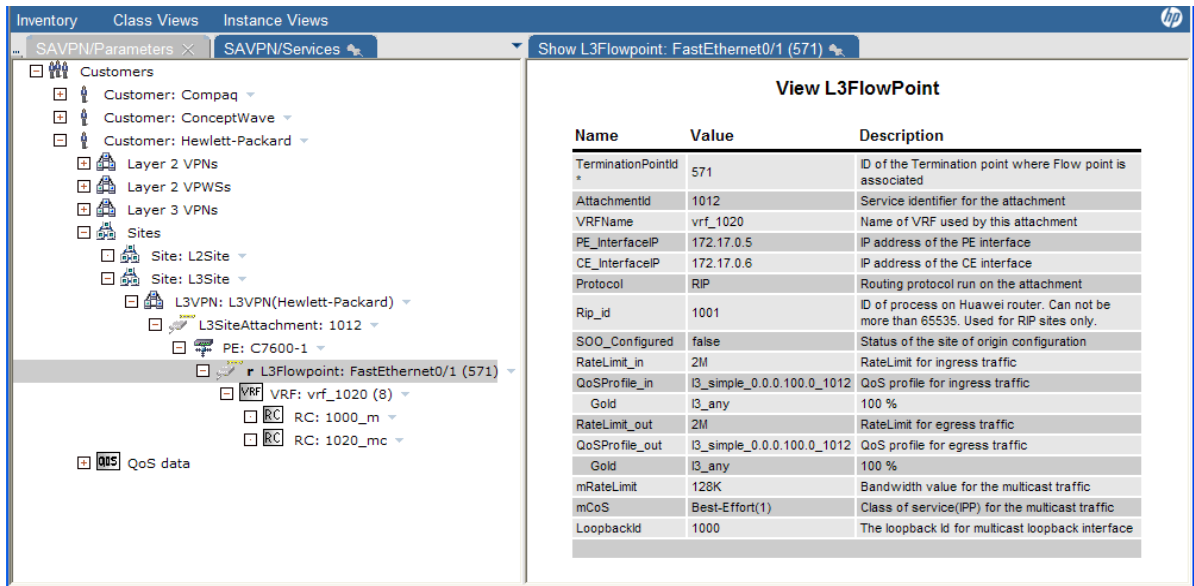- Select the SiteAttachment object corresponding to the modified attachment circuit to view the access flow parameters.

- Note the mVPN access flow related parameters: **MDTData, Loopback address** and **RP** status.
- The site specific multicast parameters **mRateLimit** and **mCoS** may be observed on the **L3Flowpoint** object

7-4-6 Modify Static Routes of Layer 3 VPN Site Attachment Service

The VPN_SVP allows you to configure static routes on the customer site attachment circuits. Static routes allow a customer site to announce its network prefixes to other sites in the VPN without itself participating in routing control exchanges with the provider's network. Static routes may be configured exclusively or in addition to an existing routing protocol, e.g. OSPF.

Below is illustrated how to add *Static routes* associated a Site attachment circuit:

- To modify *Static routes*, select in the *Existing* Services area of the *Customer Services* form, the *Modify Service* ![icon] icon next to the service type *layer3-Attachment* of the Site attachment you intend to modify.

- Select *Add static routes* from the drop-down list for the field *parameter to modify*.
  You may add several route entries by selecting the More entries link.

- Select the **Submit** ![icon] button. Service Activator will proceed with the activation and configure the specified static routes service

Your request to modify the service will be forwarded to Service Activator. The service request will start a workflow in Service Activator which will manage the activation of the router and will change the router configuration for the given service without any network operator interactions needed.

To view the result of modifying *Static routes* of an L3 VPN Site in Service Activator:

● Log in to Service Activator and navigate to the Inventory GUI window.

● Select the *SAVPN/Services* view, locate your customer and expand its *Layer 3 VPN Sites* branch where you select the site which contains the site attachment which was modified above to view the site parameters

An existing static route can also be removed from a customer site attachment circuit.

Below steps illustrates how to Remove Static routes associated a Site attachment circuit:

● To modify *Static routes*, select in the *Existing* Services area of the *Customer Services* form, the *Modify Service* icon next to the service type *layer3-Attachment* of the Site attachment you intend to modify.

● Select *Remove static routes* from the drop-down list for the field *parameter to modify*. You may select one or more route entries by selecting the 'delete route' check box.

- Once the check boxes have been selected for the routes to be removed, select the **Submit** button. Service Activator will proceed with the activation and reconfigure the specified static routes service with remaining static routes.

7-4-7 Add Protection to a Layer 3 VPN Site Service

When a L3 VPN site attachment has been activated with BGP as the PE-CE routing protocol, it is possibly to add an additional protection attachment to the existing attachment.

The protection attachment will be terminated on a physically different provider edge device than what was used for the initial attachment.

To add protection, follow these steps:

- Log in to CRM Portal.

- Find your customer e.g. *Giga-tronics Inc.* and open the *Customer Services* form. (See also 4-3 Search for Customer Records for navigation instructions).

- In the *Existing* Services area of the *Customer Services* form, identify the L3 VPN site that you want to add protection for. E.g. *BigSite1* below.

NOTE: The '*layer3-Protection*' **Subservice** is available for BGP sites only.

	Id △	Name	State	Type	Submit date	Action	Subservices	
	1075	LargeVPN	Ok	layer3-VPN	14/11/2010	⟳✗▨	layer3-Site ▾	→
⊟	1078	bigSite2	Ok	Site	14/11/2010	⟳▨	layer3-Protection ▾	→
	1079	-	Ok	layer3-Attachment	14/11/2010	⟳✗▨		→
⊟	1076	bigSite1	Ok	Site	14/11/2010	⟳▨	layer3-Protection ▾	→
	1077	-	PE Ok	layer3-Attachment	14/11/2010	⟳✗▨	Start CE activation	→

Existing services (11)   Page 1/2   Go to page 1   First   Previous   Next   Last

---

- Select the **Submit** [→] button to requests a **Subservice** of type '*layer3-Protection*' as indicated in the form.

- This brings up the *Create Services* form in which you must enter the l3-Site service related parameters. Note, that certain site related parameters specified when the initial attachment was requested can not be changed, as this is the same site getting an additional attachment.

- You may specify other **QoS** related parameters for this site, a different **activation scope** and optionally another customer ASN for this BGP peering, although the default provided may probably be OK.

Service information	
Site name (id)	bigSite1 (1076)
layer3-Attachment id	1080
region	Denmark
location	Copenhagen
rate limit	1Mbps ▾
QoS profile	l3_simple_0.0.0.0.100 ▾
Platinum	l3_any 100 ▾ 1Mbps
site connectivity type	mesh
managed CE routers	false
activation scope	PE only ▾
PE-CE address pool	PE-CE Default ▾
PE-CE routing	BGP
customer ASN	1234
Scheduling information	
start time	▦ Reset
end time	▦ Reset

Select the **Submit** ➡ button to forward the site service request to Service Activator. You will be returned to the *Customer Services* form where you will find the new site attachment entry being added to the selected VPN service.

Adding protection to an existing site requires the network operator to provide the edge device details. As described in section 7-2-1 jobs related to the selection of provider edge device and the port/interface are posted on the **add_l3_site_pe** queue. Follow these steps to activate your edge routers for the L3 service requested in 7-1-2 Add Layer3 VPN Sites:

- Log in to Service Activator.
- Select *Jobs* from the *Work Area* menu in the left navigation pane. This will open the *Active Jobs* form.
- Go to the **add_l3_site_pe** tab and right click on the selected job.

Active Jobs

| add_l3_site_pe(1) | controller_queue(1) | failed_jobs(1) | Running Jobs | Scheduled Jobs | | | | | |

| | | | | Retrieve limited jobs ▾ | | | Results 1 - 1 |

VPN Info	Service Id	Workflow	Status	Start Time	Post Time	Step	Node Description
Customer:"Giga-tronics Inc. (81)" VPN:"LargeVPN (1120)" Site:"bigSite1 (1124)"	1164	L3VPN_ReserveResource	Waiting	Aug 14, 2008 11:37:25 AM	Aug 14, 2008 11:37:25 AM	Select_PE_Router_And_If	Select the PE router and the interface on the selected PE router.

Interact with Job
Stop Job

- Select **Interact with Job** from the pop-up menu.

- This provides the usual interface to the network operator for the selection of the provider edge device.

- The **Select Router** list of available edge devices will include the list of available devices except the device that was used for the initial attachment.

- Select the desired edge device among the ones available for this location presented in **Select Router** list and select the desired interface from the **Select Interface** list

- Select the **Submit** button and HPSA will continue with the activation and configuration of the selected port on the selected device(s).

To view the result of adding **protection** in the CRM Portal, follow these steps:

- Log in to CRM Portal.

- Find your customer e.g. *Giga-tronics Inc.* and open the *Customer Services* form.

You may observe that two layer3-Attachment services are present for the site, one with Type layer3-Attachment and another with Type layer3-Protection. Also, there are now no further **Subservices** available for the site (e.g. *bigSite1*).

To view the result of adding **Protection** to an L3 VPN Site in HPSA, follow these steps:

- Log in to Service Activator and navigate to the *Inventory* GUI window.

- Select the *SAVPN/Services* view and expand the *Customers* branch.

- Locate your customer *Giga-tronics Inc* and expand its branch.

- Expand the *Layer 3 VPN Sites* branch.

- Expand the branch of the site you added protection to, e.g. bigSite1

You may observe that a pair of SiteAttachment objects now exists for the site. One represents the initial attachment; the other represents the protection attachment.

These two attachments are otherwise equal in status, i.e. there is e.g. no primary/backup relation between the two attachments.

8 Additional Facilities

8-1 Enable/Disable of Services

Services that you have requested and created as described in the previous sections, enters by default into activated state where the service is enabled and available for use. And the services stay active if otherwise not specified as e.g. a timed service as described in section 8-2

Removing services also frees the resources allocated to the services and these resources then becomes available for other services.

Occasionally, it may be desirable to disable a service without freeing the allocated resources. Then, it will be easy to re-enable such services without changing the setup or the associated resources. This could e.g. be in cases some network repair work is to be made and there is a planned outage of some services or it could e.g. due to missing payment of the services.

After the issues are back in order, the services may then be re-enabled as a simple operation.

VPN_SVP supports these functions as single-click operations via the CRM Portal GUI.

● Log in to CRM Portal.

● Find your customer open the *Customer Services* form. (See also 4-3 Search for Customer Records for navigation instructions).

● In the *Existing* Services area of the *Customer Services* form, select the *Disable service* icon next to the service you intend to disable. You may select the *Disable service* operation on VPNs or on single sites services.

● When a service has been disabled the State will be displayed as *Disabled* and the only Action available will be *Enable service*

	Id ▲	Name	State	Type	Submit date	Action	Subservices	
	1044	L2P2P	Ok	layer2-VPWS	01/09/2008		No subservices	
	1023	L3VPN	Disabled	layer3-VPN	29/08/2008			
+	1026	L3Site2	Disabled	layer3-Site	29/08/2008			
+	1024	L3Site1	Disabled	layer3-Site	29/08/2008			

Existing services (6)   Page 1/1   Go to page 1   First Previous Next Last

---

NOTE: When you select *Disable service* of a VPN, the service request will automatically iterate through all the site services in the VPN and disable these individually.

● Enabling or resuming services again is similar to the above steps, only now the Enable service icon should be selected.

NOTE: Disabling/Enabling of services is done by controlling the administrative state of the PE interface on which the service is terminated.

8-2 Timed Services

VPN_SVP supports timed services and scheduling of services request. Not all request types supports scheduling, as the request types that involve no device activation does not make sense to request as scheduled.

All requests for timed services are initiated from the CRM Portal. All site creation requests support the optional specification of **start time** and **end time** in the **Scheduling information** section:

Scheduling information			
start time	2008.08.15 14:04	▦	*Reset*
end time	2008.08.18 14:05	▦	*Reset*
Comments			

NOTE: Leaving **start time** blank means *now*, leaving **end time** blank means *never*.

The request is submitted as usual and the **State** displayed in the CRM Portal view is e.g. updated to *'PE Wait Start* Time' (e.g. site T1 below)

It is also possible to only specify an **end time** enabling you to create a site service *now* but with predetermined termination date. This could e.g. be for promotion or test purposes. After the network operator has assigned the edge device resources to the requested service, its termination request will then enter as a scheduled request and the **State** displayed in CRM portal will be updated *to 'PE Wait End Time'*

Existing services (8)		Page 1/1		Go to page	1	First	Previous	Next	Last

	Id ▲	Name	State	Type	Submit date	Action	Subservices	
	1165	ScheduledServices	Ok	layer3-VPN	14/08/2008	⟲✗▦	layer3-Site ▾	➡
⊟	1168	T2	Ok	layer3-Site	14/08/2008	None		
	1169	-	PE Ok Wait End Time	layer3-Attachment	14/08/2008	None		
⊟	1166	T1	Ok	layer3-Site	14/08/2008	None		
	1167	-	PE Wait Start Time	layer3-Attachment	14/08/2008	None		

In HPSA the jobs awaiting their activation time are visible in the **Scheduled Jobs** tab. Scheduled jobs in HPSA are persisted to the database and consume very little resources while waiting.

Active Jobs

controller_queue(3) | failed_jobs(1) | Running Jobs | **Scheduled Jobs**

Retrieve limited jobs ▼   Results 1 - 2

VPN Info	Service Id	Workflow	Status	Start Time	Repeating Period	Group Id	Description
Action:"add" Deaction:"remove" Service:"L3SiteAttachment" Service_id:"1167"	1167	TimedServiceController	WAIT_ACTIVATION	Aug 15, 2008 2:04:00 PM		3755	Action:"add" Deaction:"remove" Service:"L3SiteAttachment" Service_id:"1167"
Action:"add" Deaction:"remove" Service:"L3SiteAttachment" Service_id:"1169"	1169	TimedServiceController	WAIT_DEACTIVATION	Aug 14, 2008 2:50:00 PM		3759	Action:"add" Deaction:"remove" Service:"L3SiteAttachment" Service_id:"1169"

When the end time is reached the deactivation requests enters a confirmation queue to allow the network operator to confirm the deletion of the scheduled service.

While the job is awaiting the operator confirmation the CRM Portal State is updated to '*Sched Delete Confirm'*

VPN_SVP also supports scheduled modifications of the **rate limit** values and additionally, such modification may be requested as periodic or recurrent modifications. You may use this to e.g. increase the available site **rate limit** at regular intervals in time, e.g. each Monday from 14:00 to 20:00 if a customer has specific needs for extra bandwidth at regular intervals, e.g. for back-up purposes.

When you select the Modify operation as described e.g. in section 7-4-2 observe the **Scheduling information** section now available. Besides the **start time** and **end time** fields it also provides for specifying the modification to be **periodic,** the **repeat** period and a termination date for the periodic modifications **until** which the process should continue.

Service information

layer3-AttachmentId	T2-layer3-Attachment (1170)
parameter to modify	Rate limit ▼
rate limit	10Mbps ▼

Scheduling information

start time	2008.08.14 15:30	Reset
end time	2008.08.14 15:40	Reset
periodic?	Yes ▼	
repeat	Daily ▼	
until	2008.08.18 15:30	Reset

The request is submitted as usual and the **State** displayed in the CRM Portal view is regularly updated to *'Periodic Modify PE Wait Start'* and *'Periodic Modify PE Wait End'* corresponding to the progress of the requested schedule.

Limited interaction with ongoing scheduled requests is possible for the network operator using the HPSA GUI. This allows you to change the time for the next activation occurrence and/or to request the schedule to be stopped (terminated).

Follow these steps to stop an ongoing scheduled activation

- Log in to Service Activator.
- Select *Jobs* from the *Work Area* menu in the left navigation pane. This will open the *Active Jobs* form.
- Go to the **Sheduled Jobs** tab to locate the jobs to interact with and right click on the selected job. This will open an additional pop-up menu.

- Select **Modify Job** from the pop-up menu. This brings up the following form

- Modify the **Status** to STOP to request the schedule to be terminated
- Optionally change the **Schedule Time** for its next scheduling which is when the modify Status will be examined.
- Select the **Submit** button to modify the job
- The view will now reflect the requested changes and the job will terminate at the specified time (**start time** in the Scheduled Jobs view)

Likewise you may stop an ongoing periodic job, but only when the job is in **Status** *WAIT_ACTIVATION* so to assure we terminate the schedule at the service's initial value.

8-3 Aggregated Interfaces

VPN_SVP supports aggregation (or bundling) of interfaces. This allows you to appoint multiple physical interfaces on a PE device that should be bundled together and be represented via a single logical interface. You may do this to achieve e.g. higher bandwidth or better redundancy.

The interface types/encapsulations that are supported for aggregation covers:

- Link aggregation of Ethernet interfaces
- FrameRelay bundling
- PPP multi-link

You must create an aggregated interface *before* you may select it for service provisioning.

VPN_SVP supports bundling through a generic interface for the network operator. To create bundled interfaces follow these steps:

- In the *Inventory*, select the *SAVPN/Equipment* view.
- Expand a region branch and locate your network.
- Expand the network branch and **PE routers** branch to locate the router to be selected for the creation of an aggregated interface
- Right-click and select the **Create aggregated interfaces** action. This will open the *Create Aggregated Router Interface* form.
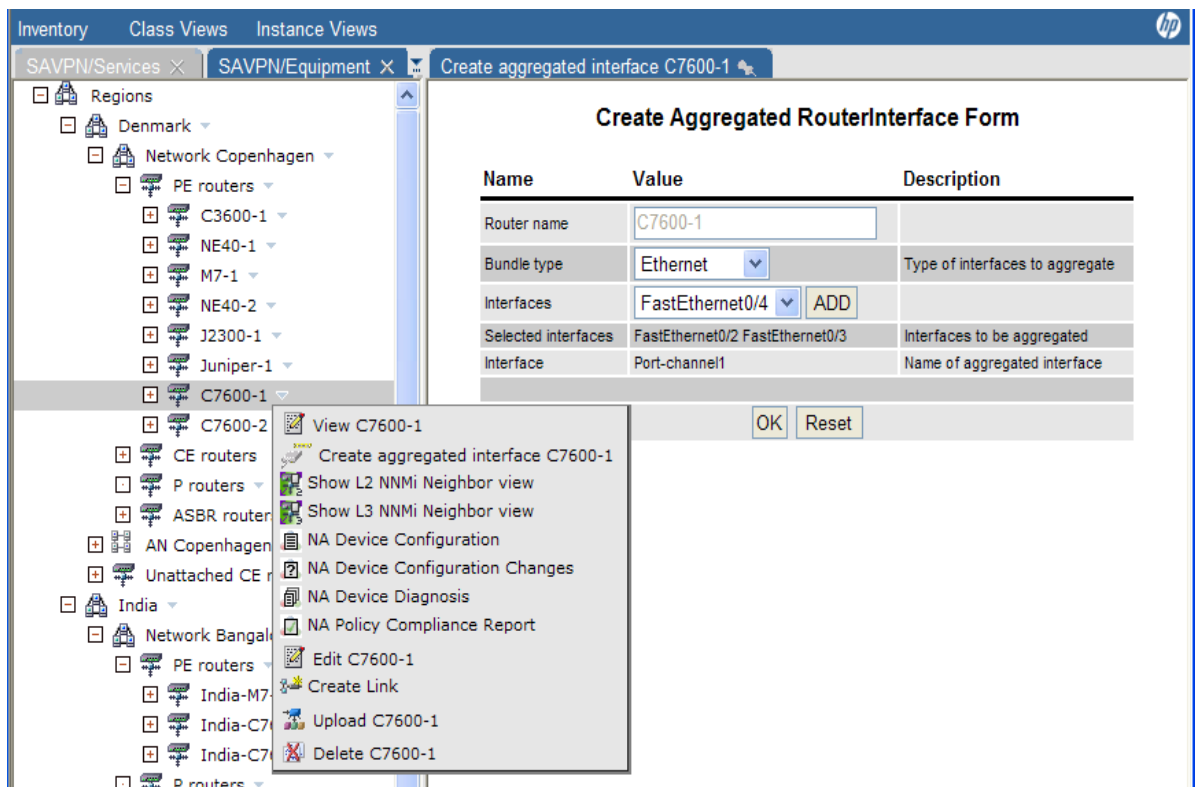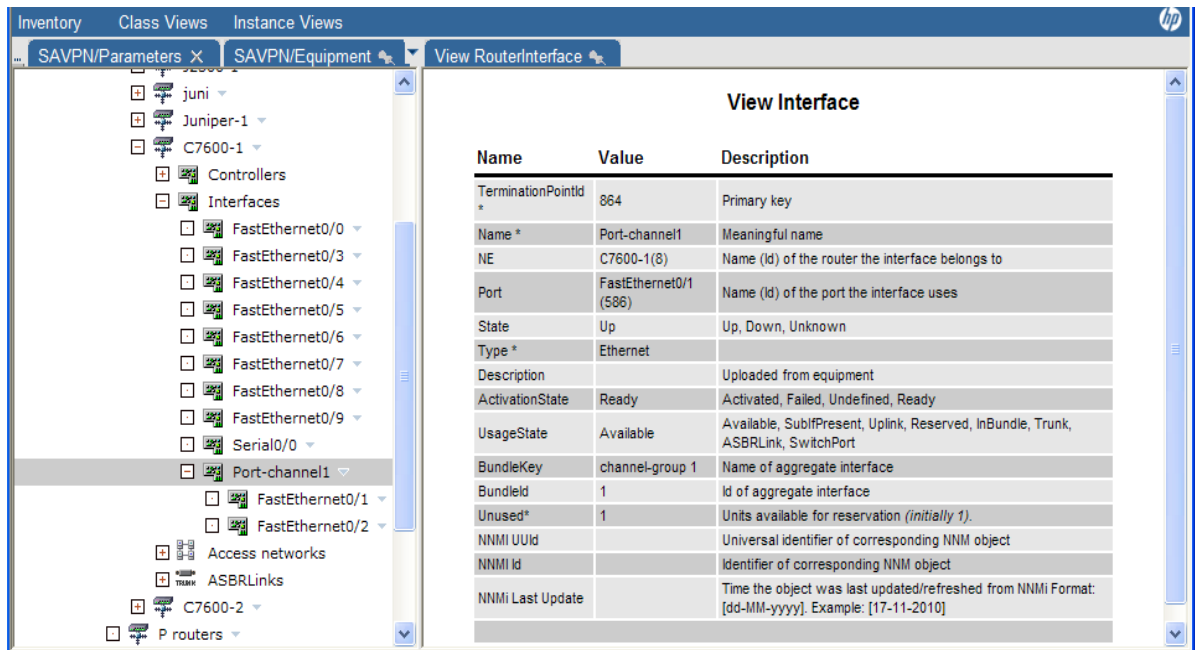
- You may select the **Bundle type**, e.g. Ethernet, and the selection list **Interfaces** will allow you to select among matching and free Ethernet interfaces to build up your aggregated interface. If you select FrameRelay or PPP, free interfaces of type Serial will be proposed.
- You select each physical interface by selecting **ADD** button for each. Note that the list **Selected interfaces** gets populated with the interfaces you have selected so far. Also note that the aggregated interface name gets display in the **Interface** field. You may want to note this name for later reference when provisioning a service.

- When all the desired physical interfaces have been added, press **OK** to submit your requests.

HPSA will now execute a WF that configures the selected PE router to create the aggregated interface according to the selections made and updates the inventory database correspondingly.

You may observe the created interface under the Interfaces branch on the selected PE router.

You should follow the same above steps to create a type multilink PPP or Frame Relay interface.

NOTE: After an aggregated interface is used for a service, it may not be possible to change its configuration with respect to its member interface (i.e. the physical interfaces that constitute the bundle).

NOTE: Deleting a free aggregated interface is done using the delete action on the interface. This will configure the device accordingly and remove the aggregated interface from Inventory and free its member interfaces.

Following are the various aggregated interfaces created for different Bundle Types chosen.

Bundle Type	Vendor	Aggregated Interface Name
Ethernet	Cisco	Port-Channel
PPP	Cisco	Multilink
FrameRelay	Cisco	MFR
Ethernet	Juniper	ae
PPP	Juniper	ml
FrameRelay	Juniper	ml

8-4 Channelized Interfaces

VPN_SVP supports channelization of E1 or SONET/SDH controller interfaces. This allows you to create logical serial interfaces that are constructed from a number of time-slots on an E1 or STM1/STM4 type of multiplexed interface and which bandwidth may be tailored to the needs of the service.

A Channelized interfaces may be created "just in time" by using the **Create Interface** button in the *Select_PE_Router_And_If* form or from the Inventory GUI ahead of the provisioning task.

Follow these step the create a channelized from the *Select_PE_Router_And_If* form

- Log in to Service Activator.

- Select *Jobs* from the *Work Area* menu in the left navigation pane. This will open the *Active Jobs* form.

- Go to the **add_l3_site_pe** tab to locate the jobs to interact with and right click on the selected job. This will open an additional pop-up menu.

- Select **Interact with Job** from the pop-up menu

- This provides the interface to the network operator for the selection of the provider edge device

- Select the desired device from the **Select Router** list. Note, when the selected device contains Controllers, and extra **Create Interface** button appears in the form

- Select the **Create Interface** button in the form as you realize that for this specific service a channelized interface must be used and it has not yet been created

The following form will appear

- In the form you may select the desired Controller on which the channelized interface should be created. Select e.g. the SONET 4/0/0 controller and then select the button **Submit** and the following expanded form will appear

ChannelizedInterface Creation Form

Name	Value	Description
Timeslots	16	Number of required 64Kbps time slots
Contiguoues	☑	Time slots allocation method
Interface	Serial4/0/0.1/1/1/2:0	Name of created router interface
Channel	0	Allocated channel group for router interface
Framing	crc4 ▾	Specifies if the interface is unframed
Clock Source	internal ▾	Interface clock source
Multiplexing	au4 tug3 tug2 e1 timeslots	
	1 ▾ 1 ▾ 1 ▾ 2 ▾ 1-16 ▾	
	Select interface	
	OK Reset	

Submit

- Notice, that the first available multiplex indexes (**au4, tug3, tug2**) for the SONET controller and an **e1** group have all been populated.
- Also notice, that the requested Ratelimit in the service request (1Mb) has been used to select 16 timeslots to provide the requested bandwidth.
- Finally, notice that the resulting serial interface name is provided **Interface** field
- If the suggested parameters needs to be changed, you may do that and re-select the button **Select Interface** to update the form
- When all parameters have been finalized, create the interface by selecting the **Submit** button

HPSA will now execute a WF that configures the selected controller on the selected edge device to create the channelized interface according to the selections made and updates the inventory database correspondingly.

You may observe the created interface under the Interfaces branch on the selected PE router.

Follow these steps to create a channelized interface from the Inventory GUI ahead of the provisioning task.

- In the *Inventory*, select the *SAVPN/Equipment* view.

- Expand a region branch and locate your network.

- Expand the network branch and **PE routers** branch to locate the router to be selected for the creation of an aggregated interface

- Expand the Controllers branch and select the desired controller to host the channelized interface

- Right-click and select the 🖋 **Create channelized interface** action. This will open the *ChannelizedInterface Creation* form as above, only now you have to provide the number of timeslots (**SlotsNumber**).

- To complete the process, you must follow basically the same procedure as described above when initiated from the *Select_PE_Router_And_If* form.

NOTE: Deleting a free channelized interface is done using the delete action on the interface. This will configure the device accordingly and remove the channelized interface from Inventory.

8-5 Work-order Distribution

VPN_SVP supports distribution of Work-orders by e.g. email. This may help the provider integrating and organizing the activation process of managed CE VPN sites with field technicians and/or 3rd-party technicians. These personnel perform the actual CE router installation and pre-configuration possibly at the customer's premises and may not have direct access to the VPN_SVP GUIs and interaction forms.

Although the VPN_SVP does not support managed L2 VPN CE (Customer Edge) devices, L2 VPN Site work-orders are yet generated to provide help in setting up the CE device

8-5-1 Work-order Distribution

You may initialize Work-order distribution by following these steps:

- Log in to Service Activator.
- Select the **Inventory** from the left pane menu.
- Select the *SAVPN/Parameters* view.
- Expand the **SP Parameters** branch.
- Locate the **Workorder distribution** object
- Right-click the **Workorder distribution** and select the ▦ **Edit Workorder distribution** action
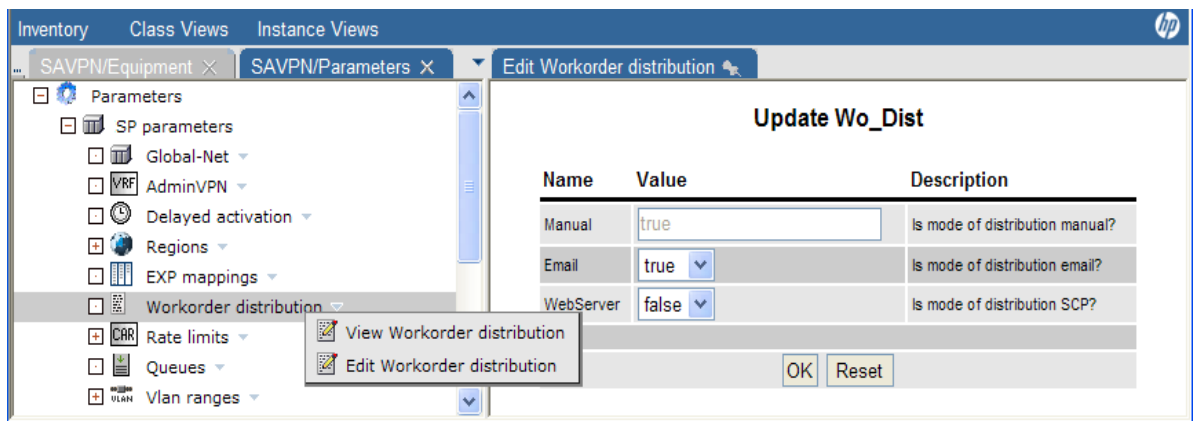
- Add Email distribution to the set of supported distribution methods by selecting **Email** *true.* Note that **WebServer** distribution method is not yet supported. Note, that the Manual mode is always enabled, which means that a copy of the generated work-order always is saved in the database and accessible from HPSA left navigation **Work-orders** menu as described in section 7-2-2-3

You have now added email distribution mode to the work-order distribution mechanisms.

You must now create a temporary storage for the work-orders that must be distributed to external recipients. You may follow these steps to create a *queue* as temporary storage for these work-orders:

- Log in to Service Activator.
- Select the **Inventory** from the left pane menu.
- Select the *SAVPN/Parameters* view.
- Expand the **SP Parameters** branch.
- Locate the **Queues** branch
- Right-click the **Queues** and select ▦ **Create Queue** action
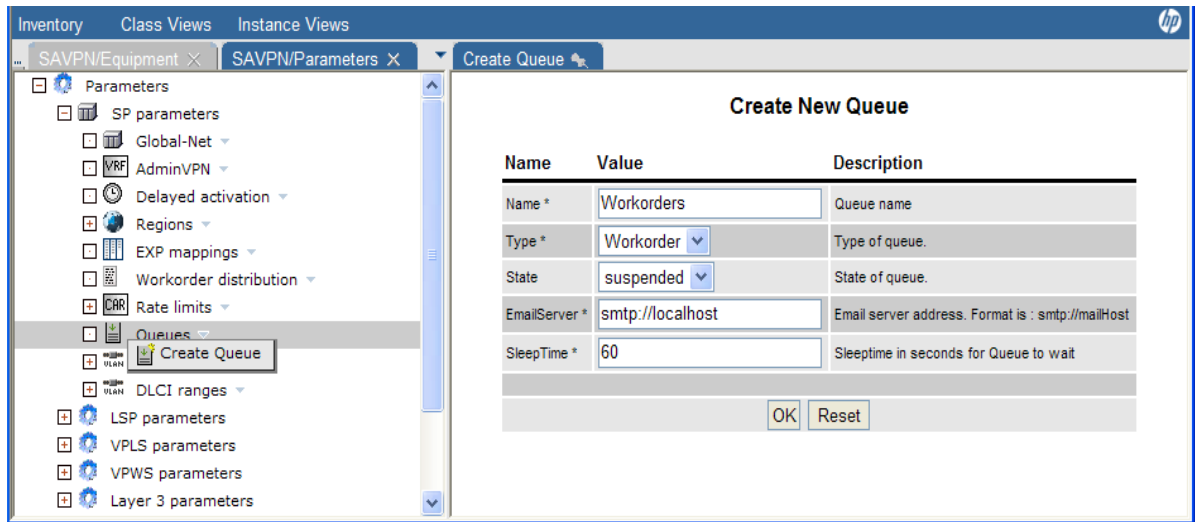
- Fill in the form providing **Name** as e.g. *Workorders*. Select the queue **Type** as *Workorder,* **State** as *suspended*. You may change this later as described below.

- Provide the address of your **Email server** in the URL format as indicated. This is the external SMTP server that emails will be submitted to and relayed via towards the final recipient.

- Press the **OK** button to submit the information

You have now created a queue in the database that the VPN_SVP provisioning process may submit information (work-orders) onto. Currently, the built-in work-order distribution mechanism submits the work-orders onto queues of Type Workorder and which are not in State disabled.

The created queue provides a temporary storage for the work-orders and the service activation process will commence immediately after submitting a work-order. This decouples the service activation process effectively from the distribution process.

The queue is served by a scheduled server work-flow that de-queues submitted requests one-by-one and sends these via the above configured SMTP server. This will only take place when the state of the queue is active.

Hence, when the State is suspended, work-order requests will be submitted onto the queue and saved there, but the distribution process will not serve the queue and distribute any requests.

When a request is successfully sent to the configured external SMTP server, it is removed from the queue and the next request will be attempted.

To enable the distribution of work-orders you must set the queue State to active. Follow these steps to do that:

- Locate the *Workorders* queue you created above
- Right-click the queue and select the ↻ **Resume Workorders** action
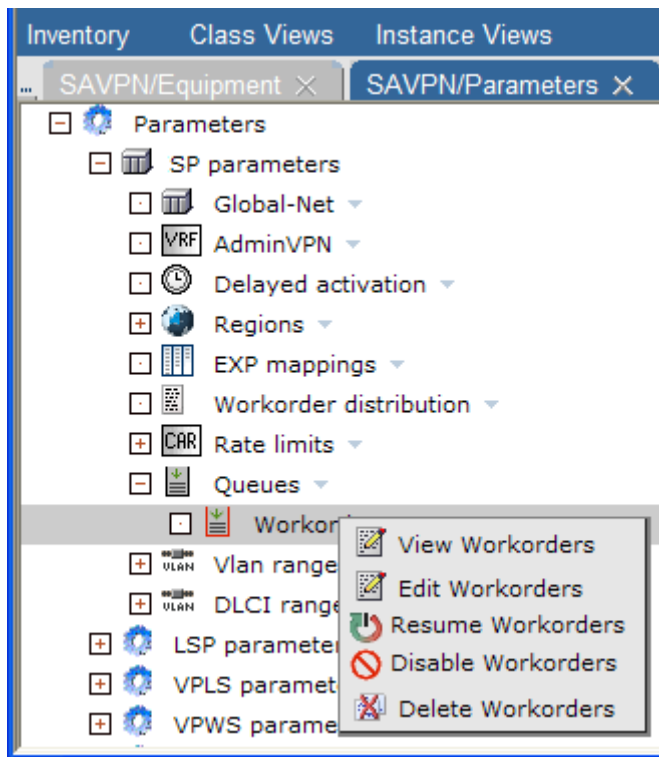
The State of Workorders queue will now be set to active and the distribution process started. You may later Suspend or even Disable the queue if so desired.

NOTE: If you Disable the queue, the requests submitted so far and not yet distributed, will also be deleted.

You still need one final configuration step before work-order distribution is fully configured: The recipient address for the work-orders needs to be provided.

VPN_SVP supports specifying per Region and optionally also per Location, recipient's email address.

To configure Work-order recipient email addresses, follow these steps:

- Log in to Service Activator.
- Select the **Inventory** from the left pane menu.
- Select the *SAVPN/Parameters* view.
- Expand the **SP Parameters** branch.
- Locate the **Regions** branch
- Select the desired Region, e.g. *Denmark* and expand
- Select the action ▤ **CreateWorkorderURL** on the **WODistribution** object.
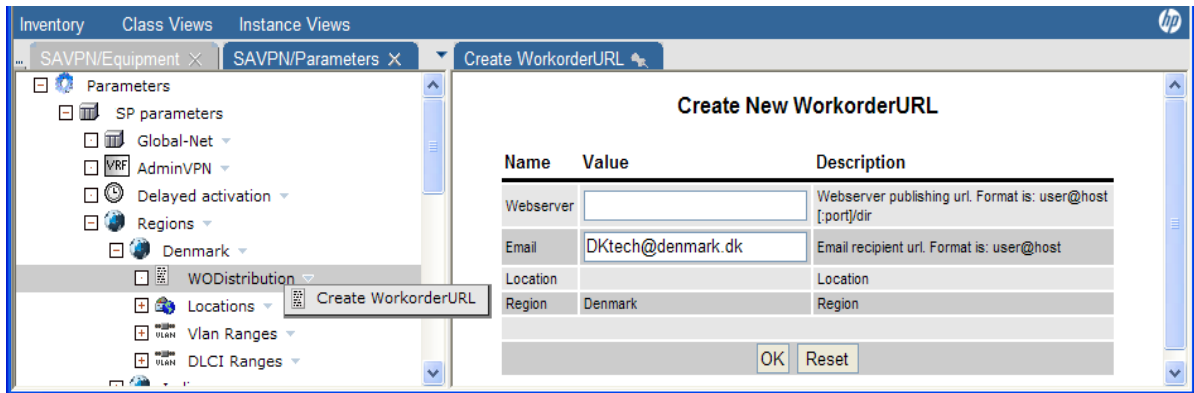
- Fill in the **Email** field representing the recipient's email address.

NOTE: **Webserver** publishing feature is not currently supported.

- Similarly, you may specify a more dedicated email recipient address for any of the Locations in a Region by expanding the desired Location branch and configuring the **WODistribution** object there.

VPN_SVP will, when submitting a Work-order to the Workorders queue, use a Location specific recipient address if it is defined, otherwise the Region level address will be used, if that has been is defined.

NOTE: Distribution of layer3 Work-orders for *Managed* CE routers will use this Region/Location based recipient address whereas Work-orders for *Un-managed* CE routers will be send to the email address of the customer's contact person, if that has been specified.

---

9   Reporting

This chapter describes the Reports tool available in the VPN_SVP. As described in Chapter 3, the VPN_SVP support a detailed view of *Services, Equipment,* and *Parameters* via the Inventory GUI and additional examples of these views are described throughout the previous chapters. The Inventory GUI is hierarchical in nature and therefore certain types of information are not readily available. The Reports tool provides a set of predefined views that allows you to extract information that is somewhat orthogonal to the Inventory views.

The Reporter tool provides three basic reports: 'Executive Summary', 'Services per PE' and 'Bandwidth per PE' which are all described in detail in the following sections.

Follow these steps to enter the Reports tool:

- Log in to Service Activator.

- Select *Reports* from the *Tools* menu.
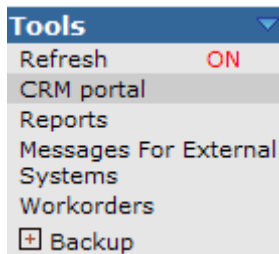
- This will open the *Types of Reports* overview

Types Of Reports

Report Name	Description
Executive Summary Report	Summary report of the number of customers created or deleted and services created or modified in selected time-frame.
Services per PE Report	Report of the customers and the services corresponding to each customer residing on a specific PE.
Bandwidth Accounting Report	Report of the physical bandwidth, committed bandwidth and available physical bandwidth on a specific PE.

- Once in the *Types of Reports* window, select the report you desire from the **Report Name** *list*

9-1 Executive Summary Report

When you have selected the Executive Summary report, a window will appear that allows you to enter the desired time-frame of the report.

Executive Summary Report

Select Time-Frame		
Select Time-Frame	1 month ▼	
		Submit

1 month
2 months
3 months
4 months
5 months
6 months
1 year
2 years
3 years
4 years
5 years
All

- You may select a period from 1 month to 5 years or the total time that the system has been running.

- Select **Submit** to generate the Executive Summary Report

Executive Summary Report

Time-Frame: 1 months   **Mon Aug 25 10:32:58 CEST 2008**

Customers		
Added	Deleted	Active
4	2	4

Services			
Type	Added	Modified	Total
L3Site	12	2	12
L2Site	2	0	2
L2VPWS	1	0	1

Print Save

The report shows you the total number of Customers that have come or left your VPN business as well as the total number of active Customers. Additionally the report adds up the total number of sites according to type that have been added or modified within the selected time-frame.

9-2 Services per PE Report

When you select the Services per PE Report, a window will appear that allows you to select the desired PE for the reporting.

Services per PE Report

Select PE	
Region	Denmark ▾
Location	Copenhagen ▾
Routers	C3600-1 ▾
	Submit

- Select **Region** and **Location** and finally the PE **router**
- Select **Submit** to generate the Services per PE Report

Services per PE Report

Mon Aug 25 10:41:36 CEST 2008

PE Router Details		
PE Router Name	Network Element Id	Management IP
C7600-1	8	15.76.223.1

Customer Details Report							
Customer Name	Id	Contact Person	Service			VPN	
Giga-tronics Inc.	81	John Smith	Name	Id	Type	Name	Id
			Copenhagen	1247	VPWSSite	CPH-STK	1246
			GigaEthSite1	1241	L2Site	GigaL2VPN	1240
			BO	1057	L3Site	Finance	1054
			bigSite1	1124	L3Site	LargeVPN	1120
Customer Name	Id	Contact Person	Service			VPN	
Baldor Electric Company	21	John Doe	Name	Id	Type	Name	Id
			Dev2	1049	L3Site	Research	1163
			T1	1180	L3Site	ScheduledServices	1165

Print   Save

The report provides an overview of the customers and their services provisioned on a particular PE router.

9-3 Bandwidth Accounting Report

When you select the Bandwidth Accounting Report, a window will appear similar to the window above in section 9-2 that allows you to select the desired PE for the reporting.

- You select the **Region** and **Location** and finally the PE **router**
- Select **Submit** to generate the Bandwidth Accounting Report

Bandwidth Accounting Report

NE Details				Physical-Bandwidth		
Router Name	NE Id	Management IP	Committed Bandwidth	Customer-Facing	Core-Facing	Available
C7600-1	8	15.76.223.1	8960	1139216	0	439216

Unit of Bandwidth: kbps

Interface Level Bandwidth-Summary Report								
Interface Type	Number				Committed Bandwidth	Physical-Bandwidth		
	Total	Provisioned	Reserved	Available		Customer-Facing	Core-Facing	Available
Serial	1	0	0	1	0	2000	0	2000
FastEthernet	10	5	2	3	8960	1000000	0	300000
SONET	1	0	-	1	0	129024	0	129024
E1	4	0	-	4	0	8192	0	8192

Print   Save

The report provides information about the types and number of interfaces on the selected NE router and the bandwidth provisioned on these interface types (Committed Bandwidth). The report also summarizes the total amount of customer facing bandwidth (Customer Facing) and the amount yet available on the NE (Available).

10   Problem Control

This chapter describes how VPN_SVP facilitates the handling of problems and errors that may occur when services are provisioned.

Different issues may cause the activation of a service to fail. It could be a temporary loss of connectivity to the PE router from the NOC, it could be some router problem related to the specific version of the router firmware, it could be exhaustion of different resources managed by VPN_SVP such as address pools, etc., etc.

The precise diagnosis of a particular problem may in some case require a substantial amount of work by specialized and skilled network operators and/or engineers and may in other cases be simple and straight forward to identify. Likewise the resolution of the problem may represent a substantial amount of work and could include a complete replacement of a failed PE router.

To facilitate problem handling and error recovery several tools are available in the VPN_SVP which are described in the following sections.

10-1   Error and Notification Messages

The Message queues **Errors** and **Notification** are used by the work-flows in the VPN_SVP solution to post messages that may help the operator in identifying a problem and possible also help in solving the problem.

The queues used for errors and notifications are configurable via the Inventory GUI. You may configure the queue names used by following these steps:

- Log in to Service Activator.
- Select the **Inventory** from the left pane menu.
- Select the *SAVPN/Parameters* view.
- Expand the **SP Parameters** branch.
- Locate the **Service Provider** object
- Right-click the **Service Provider** and select the ▦ **Edit Service Provider** action
- You may now enter the names you want to use for the **ErrorQueue** and **NotificationQueue** attributes

These attributes are use by the Workflows when they need to post a message.

The **Notification** queue is used to post messages that do not represent some error but rather some important or some un-usual events, that may be of importance to the operators of the system.

Below are two examples of notification messages. One is from the ErrorHandler when re-submitting a failed service requests (see section 10-2), the other represents a timed service that an operator has stopped (see section 8-2)

Messages

Errors | **Notification**

<<   <Prev   1 - 2 / 2   Next>   >>   Go

Job Id ▲	Service Id	Hostname	Workflow	Post Time	Step	Message
3168	1207	fhustedand2	ErrorHandler	Aug 5, 2008 4:10:34 PM	Re-submit message	Service Id: 1207 - Error handler re-submitted the message: db:1717
3755	1167	fhustedand2	Controller	Aug 14, 2008 3:55:00 PM	Put stopped msg	L3VPN_AddSiteAttachment Scheduler Stopped

The **Errors** queue are used to port messages that's concerned with activation failures, workflow failures or other irregular events that must be investigated by the operator.

Below are examples of two problems and the generated Error messages. The first (top) one is related to remote interaction with the **confirm_setup_ce** queue where the remote operator may have provided an illegal Service Id in the interaction form (see section 8-5-2) which generates an exception message in the Errors queue.

The second problem is related to a L3 VPN Site service request where allocation of an IP address failed due to lack of available resources. This causes a failure of the requests and it is then queued in the ErrorHandler. In the ErrorHandler the operator has failed the requests and the service request has been terminated and responded back to the CRM portal (see (see section 10-2).

Messages

| Errors | Notification |

<< <Prev **1 - 106 / 106** Next> >> [ ] Go

Workflow	Post Time ▼	Step	Message
Confirmation_CE	Aug 22, 2008 11:50:58 AM	Read service_id from DB	com.hp.ov.activator.mwfm.component.WFException: No valid message Id or identifier or job Id or host name or module name specified for job # 4,014, workflow name #Confirmation_CE in cluster node fhustedand2
Controller	Aug 22, 2008 11:45:09 AM	Put error msg	L3VPN_AddSiteAttachment Failed
ErrorHandler	Aug 22, 2008 11:45:09 AM	Fail message	Service Id: 1221 - Error handler failed the message: db:2050
ErrorHandler	Aug 22, 2008 11:44:51 AM	Enter Message	Error handler for Service Id: "1221" executed.
L3VPN_AddSiteAttachment	Aug 22, 2008 11:44:50 AM	Reserve resource Failure	Failed Reserving the resources for for serviceid: 1220
L3VPN_ReserveResource	Aug 22, 2008 11:44:49 AM	Error reserving IPNet	Error reserving IPNet address FastEthernet0/0 PoolName: PE-CE Default Mask: 255.255.255.252

10-2 Error Handling

When an error occurs in a service creation workflow, the error handler work flow receives the failure including the original service request message that was received from the CRM portal.

At the same time, the CRM portal service *State* is updated to *temporary failure.*

Follow these steps to enter handling of failed jobs for a failed service request:

- Log in to Service Activator with admin rights.
- Select *Jobs* from the *Work Area* menu in the navigation pane. This will open the *Active Jobs* form.

Active Jobs

| controller_queue(1) | failed_jobs(1) | sync(0) | Running Jobs | Scheduled Jobs |

Retrieve limited jobs [ ]   **Results 1 - 1**

VPN Info	Service Id	Workflow	Status	Start Time	Post Time	Step	Node Description
Action:"add" Service:"L3SiteAttachment" Service_id:"1002"	1002	ErrorHandler	Waiting	Jul 15, 2008 12:02:53 PM	Aug 25, 2008 9:05:35 AM	Update_Error_Handler	Check error conditions and re-submit or fail the transaction.

Interact with Job

Stop Job

Change Roles

Stop Job (Forced)

● Go to the **failed_jobs** tab to locate the failed job to interact with and right click it. This will open a pop-up menu from where you select **Interact with Job**.

The form may optionally list multiple **Activation Attempts** that has been made so far to configure the requested services but without success. For each attempt, the form allows you to inspect different pieces of information related to the service request:

   ○ **Request message**

     The service request message that was sent from the order portal (CRM Portal)

   ○ **Activation dialog**

     The generated xml activation dialog used by the CLI plug-in to configure the service

   ○ **Device dialog**

     A trace of the actual communication that took place with the external device

● You select the URL listed for **Request Message** to inspect the received service request. A simple text based view is presented. Below is illustrated part of a received service request.

```xml
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE msg SYSTEM "file:/C:/hp/OpenView/ServiceActivator/etc\config\message.dtd">

<msg Message_id="65">
  <header>
    <Service_request Skip_activation="default" Service_response="true">
      <Service_id>1069</Service_id>
      <Activation_name>add</Activation_name>
      <Deactivation_name>remove</Deactivation_name>
      <Service_name>L3SiteAttachment</Service_name>
      <Region>Denmark</Region>
    </Service_request>
    <Service_schedule>
      <StartTime/>
      <EndTime/>
    </Service_schedule>
  </header>
  <body>
    <VPNSite>
      <SiteAttachment ServiceMultiplexing="false">
        <Managed_CE_router>false</Managed_CE_router>
        <Site_Service_id>1068</Site_Service_id>
        <VPN_Service_id>1051</VPN_Service_id>
        <Location>Copenhagen</Location>
        <Comment/>
        <Attachment_name>bigsite3layer3-Attachment</Attachment_name>
        <L3SiteAttachment Type="initial-Attachment">
          <Activation_scope>PE_ONLY</Activation_scope>
          <Connectivity Type="mesh"/>
          <PE_CE_routing Customer_ASN="" OSPF_area="" Protocol="RIP">
            <Static_routes/>
          </PE_CE_routing>
          <AddressPool>PE-CE Default</AddressPool>
        </L3SiteAttachment>
      </SiteAttachment>
      <QoS>
        <Rate_limit>1M</Rate_limit>
        <QoSProfile>l3_simple_0.0.0.0.100</QoSProfile>
```

Done   Local intranet

- You may also want to inspect the xml activation dialog that Service Activator constructed for the service request and which controlled the CLI plug-in dialog with the network device. Select the link in the **Activation Dialog** column corresponding to the activation attempt you are analyzing.

Command set for the service: Add L3 Site Attachment VPN PE

Equipment name: C3600-1, Element Type: C3620, Vendor: Cisco

Description	Activation commands	Rollback commands
Connecting to Cisco device.	0e8mj+wGs94TJxRPLeYSDw==	
Privileged (enable) mode.	enable	
Privileged (enable) mode.	alJDvQoxUU30ww0xeAIDDw==	
Turn prompting off	terminal length 0	
Turn line scroll off	terminal width 256	
Configure terminal	configure terminal	
Enter (sub)Interface	interface Serial0/0	
Associate VRF with Interface	ip vrf forwarding vrf_1013	no ip vrf forwarding vrf_1013
Define hdlc encapsulation on Serial i/f	encapsulation hdlc	no encapsulation hdlc
Define IP address on i/f under vrf	ip address 172.17.0.17 255.255.255.252	no ip address 172.17.0.17 255.255.255.252
Define description on i/f	description ** HPSA VPN ** Added i/f, Customer(id): cust(1), SiteAttachment: 1021, Site name(id): Sitea(1020), Date: 2010.11.17 20:41:07	
Bring pe i/f up	no shutdown	shutdown
Delete i/f in undo		interface Serial0/0
Configure RIP CE-PE Routing	router rip	
Configure RIP address-family	address-family ipv4 vrf vrf_1013	no address-family ipv4 vrf vrf_1013
Configure RIP version 2	version 2	
Configure RIP CE-PE network	network 172.17.0.16	
Configure RIP redistribution of BGP	redistribute bgp 12345 metric transparent	router rip address-family ipv4 vrf vrf_1013 no redistrib 12345 metric transparent
Configure BGP redistribution of RIP	router bgp 12345	
Configure BGP RIP address-family	address-family ipv4 vrf vrf_1013	
Configure BGP RIP redistribution	redistribute rip	
Configure BGP redistribution of connected routes	router bgp 12345	
Configure connected BGP address-family	address-family ipv4 vrf vrf_1013	
Configure connected BGP redistribution	redistribute connected	
Create PolicyMap	policy-map l3_simple_0.0.0.0.100_in_128K	no policy-map l3_simple_0.0.0.0.100_in_128K
Define description on Policy Map	description ** HPSA VPN ** Rate Limit: 128K, Date: 2010.11.17 20:41:07	
Add Classifier to policy map	class l3_any	
Add rate-limiting	police cir 128000 bc 8000 be 8000 conform-action set-mpls-exp-transmit 5 exceed-action drop	

In this view, you may inspect to **Activation commands** to configure the service and the **Rollback commands** that will be executed if the activation experiences any errors. Also, the **Description** allows you to locate the specific command in the dialog trace that is also available.

- You may also want to inspect the actual trace of commands sent to the device and the corresponding network element responses received, to e.g. inspect any diagnostics messages from the device. Select the **Device dialog** *View* button of the activation attempt that you are investigating.

Time	Tx/Rx	Message	Description
Tue Jul 15 2008 12:02:38:758	-->		Connecting to Cisco device.
Tue Jul 15 2008 12:02:38:867	<--	User Access VerificationUsername: safePassword: ciscoc3600-1>	Connecting to Cisco device.
Tue Jul 15 2008 12:02:39:086	-->	enable	Privileged (enable) mode.
Tue Jul 15 2008 12:02:39:242	<--	Password: ciscoc3600-1#	Privileged (enable) mode.
Tue Jul 15 2008 12:02:39:242	-->	terminal length 0terminal width 256	Turn prompting off
Tue Jul 15 2008 12:02:39:461	<--	c3600-1#terminal width 256c3600-1#	Turn prompting off
Tue Jul 15 2008 12:02:39:461	-->	configure terminal	Configure terminal
Tue Jul 15 2008 12:02:39:789	<--	Enter configuration commands, one per line. End with CNTL/Z.c3600-1(config)#	Configure terminal
Tue Jul 15 2008 12:02:39:805	-->	ip vrf vrf_1000	Create VRF
Tue Jul 15 2008 12:02:40:024	<--	c3600-1(config-vrf)#	Create VRF
Tue Jul 15 2008 12:02:40:024	-->	description ** OVSA VPN ** Added vrf, Customer id: 1, VPN name(id): bigVPN (1001), Date: 2008.07.15 12:02:37	Configure VRF description
Tue Jul 15 2008 12:02:40:461	<--	c3600-1(config-vrf)#	Configure VRF description
Tue Jul 15 2008 12:02:40:461	-->	rd 12345:10020	Configure VRF rd
Tue Jul 15 2008 12:02:40:680	<--	% Cannot set RD, check if it's uniquec3600-1(config-vrf)#	Configure VRF rd
Tue Jul 15 2008 12:02:40:680	-->	no ip vrf vrf_1000	Create VRF
Tue Jul 15 2008 12:02:41:008	<--	% IP addresses from all interfaces in VRF vrf_1000 have been removedc3600-1(config)#	Create VRF
Tue Jul 15 2008 12:02:52:492	-->	exit	
Tue Jul 15 2008 12:02:52:711	<--		

In the above example trace, you may observe that the router device complains about the configured VRF using an RD value that is already in use. This indicates that e.g. some manual configuration has been made on the router behind "the back" of VPN_SVP. To rectify such an issue, the router must be examined manually and the offending VRF item may have to be deleted or modified on the router not to collide with the auto-generated version configured by VPN_SVP.

- When you have identified the cause and rectified the problem, e.g. created additional entries in an IP address pool, or rectified the router configuration, the service request may be re-submitted by selecting the **Re-submit** button. This will restart the VPN_SVP handling of the request.

- The CRM State will change to *In_progress* to inform the CRM operator about the changed status.

- If the cause of the problem is related to the service request itself, you may add a comment that will be sent back to the CRM operator when the **Fail** button is selected. This comment will be available as the *Failure description* in the CRM portal.

- The CRM Portal will change state to *Failed* and the CRM operator will have to decide on the further steps to be taken. E.g. it may be realized that the originally requested parameters were wrong in which case the failed request must be deleted and a new, with the corrected parameters, must be submitted.

- The form allows you to execute the activation request in **Skip Activation** mode. This will process the request normally, only the actual router configuration will be skipped. Only use this when you are 100% sure the router configuration is correct but the inventory of VPN_SVP must be updated correspondingly.

10-3 Delayed Activations

When an activation attempt fails with a connectivity error to the network device, the failed service request is not queued in the above **failed_jobs** queue but instead it is being automatically rescheduled for a later activation retry on the **delayed_activation_jobs** queue.

The retry properties like maximum number of retries and the time interval between retries may be managed centrally as well as on a per job basis.

If the service request does not complete successfully within its assigned number of reties, the job will fail and enter the **failed_jobs** queue and may then be handled as described above in section 10-2 .

A delayed job, will by default be associated the retry parameters defined in the Inventory→Parameters→SP parameters **Delayed activation** object. You may select the edit function and the view below should appear.

These parameters represent the default parameters associated any delayed job.

If there is a need to change the parameters on a per job basis, the job gets queued on the **delayed_activation_jobs** queue while awaiting the next retry. You may interact with delayed jobs and manage the retry parameters reties as described below.
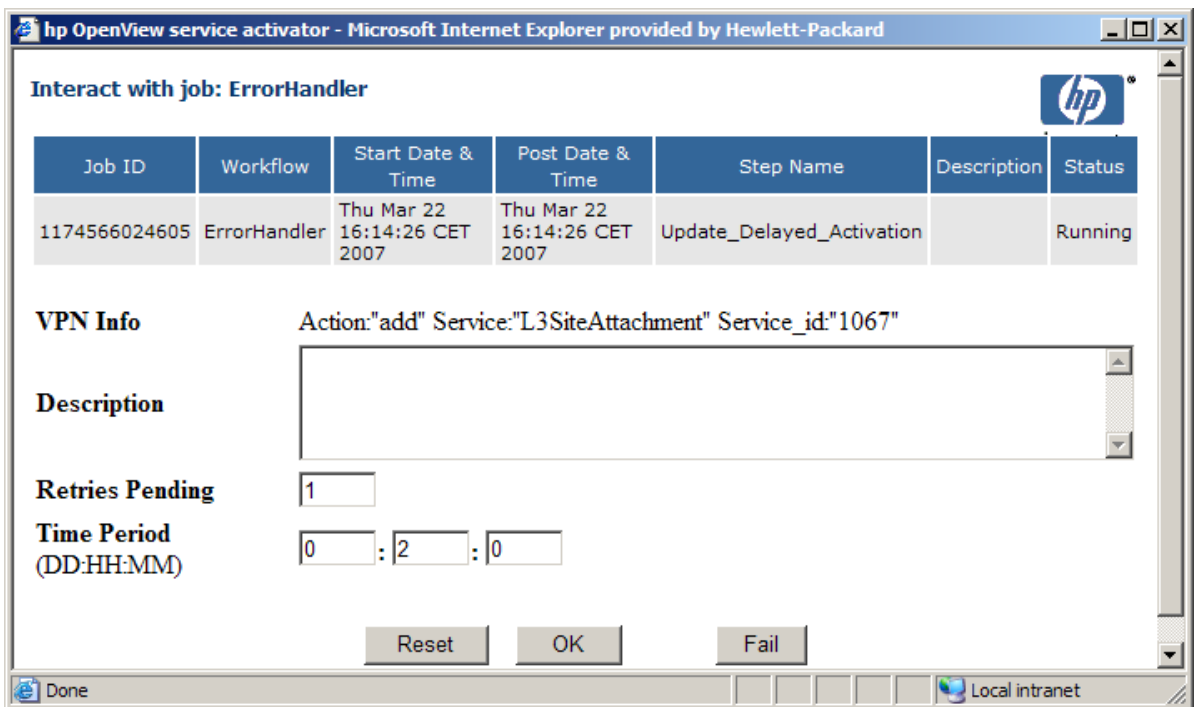
- Log in to Service Activator with admin rights.

- Select *Jobs* from the *Work Area* menu in the navigation pane. This will open the *Active Jobs* form

Active Jobs

| | controller_queue(2) | **delayed_activation_jobs(1)** | failed_jobs(1) | Running Jobs | Scheduled Jobs | |

Results 1 - 1

VPN Info	Workflow	Status	Start Time	Post Time	Step	Description	JobId ▲
Action:"add" Service:"L3SiteAttachment" Service_id:"1067"	ErrorHandler	Waiting	22-Mar-2007 16:14:26	22-Mar-2007 16:14:26	Update_Delayed_Activation		1174566024605

Interact with Job

Stop Job

Change roles

Stop Job (Forced)

- Go to the **delayed_activation_jobs** tab to locate the delayed job to interact with and right click it. This will open an additional menu.

hp OpenView service activator - Microsoft Internet Explorer provided by Hewlett-Packard

Interact with job: ErrorHandler

Job ID	Workflow	Start Date & Time	Post Date & Time	Step Name	Description	Status
1174566024605	ErrorHandler	Thu Mar 22 16:14:26 CET 2007	Thu Mar 22 16:14:26 CET 2007	Update_Delayed_Activation		Running

VPN Info   Action:"add" Service:"L3SiteAttachment" Service_id:"1067"

Description

Retries Pending   1

Time Period (DD:HH:MM)   0 : 2 : 0

Reset   OK   Fail

Done   Local intranet

- You may change the number of pending reties as well as the time interval between each retry. Note, that you may also *Fail* the job and thereby pass the job to the **failed_jobs** queue from where it may be handled as described above in section 10-2 .

10-4 Interface Recovery

In some incidents, a communication line card may fail on a router and a single or some few numbers of ports may consequently malfunction. The services that you may have provisioned on this/these ports are therefore also out of operation. This occurs not too often but when it does, the VPN_SVP provides an Interface Recovery tools that may help you swiftly migrate all the services provisioned on one port to an equivalent replacement port on the same router and which will minimize the down-time of the customer services.

The Interface Recovery tool is accessed via the Inventory GUI. Follow these steps to recover the services provisioned on an interface on your router.

- In the *Inventory Tree* window select the SAVPN/*Equipment* view.
- Expand the *Regions* branch and locate the relevant networks containing the device in failure.

- Expand the *PE routers* branch and locate e.g. the router C7600-1 with a failed port.
- Expand the interfaces branch and locate a failed interface hosting provisioned services.
- Right-click Select the **Recover services from the Router interface** action. This will open the *Interface Recovery* form:
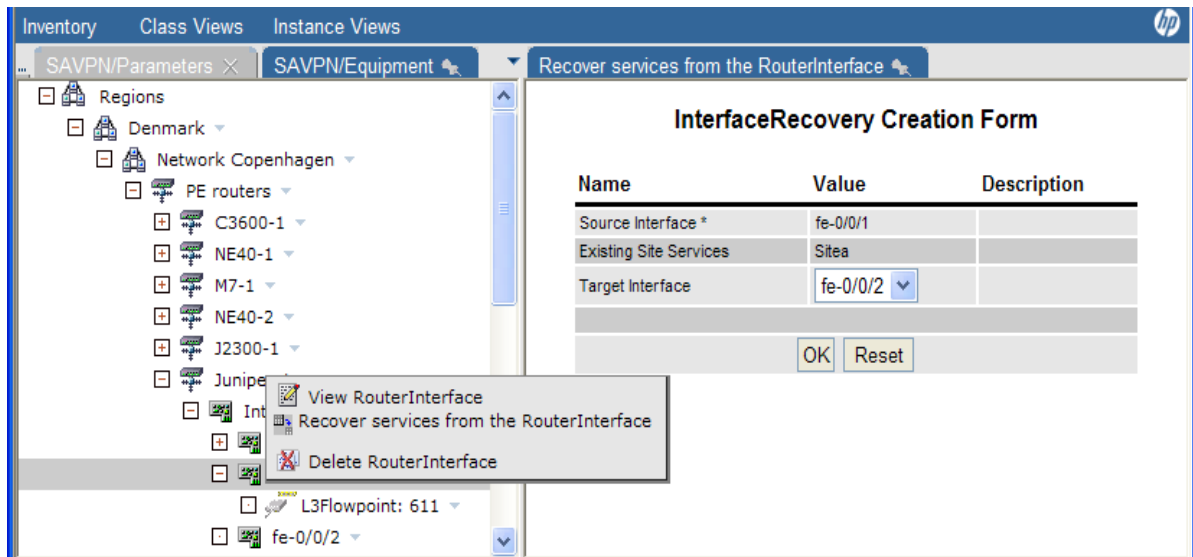
- Now, in the **Interface Recovery** form you may select the target interfaces from the selection list. This is the interface to which the services of the failed source interface should be moved
- Now select the **Ok** button to initiate the transfer of services. A progress bar will keep the status of the services migration updated.

HPSA will then create, service by service, the configuration commands to remove the service from the old failed interface and re-create the service on the new target interface. You will just have to switch the cable from the failed port or source interface to the port of new target interface. You may repeat this procedure for each failed port.

10-5 Audit Trails

When a service is successfully configured, an audit trail entry is created in the Audit system database by VPN_SVP. Each entry keeps a record of the configuration performed for that specific service activation.

These audit trails are generally useful when the need arises for analyzing which service has been activated by which operators and for which customers, etc.

But these are also particular useful when a failed PE router needs to be replaced and the already configured services on that PE router must be restored. To view an audit entry, follow this procedure:

- Log in to Service Activator with admin rights.

- Select **Audit Messages** from the *Work Area* menu in the left navigation pane. This will open the *Audit Messages* view.

- All audit entries created by VPN_SVP are of Event Type **SAVPN_LOG_EVENT**

Audit Messages

| | | | | Reset | Filter | << | < Prev | 121 - 170 / 170 | Next > | >> | | Go |

Job Id	Service Id ▲	Hostname	Workflow	Date	Event Type	Step
2984	1141	fhustedand2	ActivateConfiguration	Jul 30, 2008 4:14:03 PM	SAVPN_LOG_EVENT	L3VPN_RemoveSiteAttachment_PE
3044	1142	fhustedand2	ActivateConfiguration	Aug 1, 2008 12:39:03 PM	SAVPN_LOG_EVENT	L3VPN_RecoverSite
3000	1143	fhustedand2	ActivateConfiguration	Jul 30, 2008 4:22:44 PM	SAVPN_LOG_EVENT	L3VPN_AddSiteAttachment_PE
3047	1143	fhustedand2	ActivateConfiguration	Aug 1, 2008 12:39:04 PM	SAVPN_LOG_EVENT	L3VPN_RemoveSiteAttachment_PE
3349	1143	fhustedand2	ActivateConfiguration	Aug 11, 2008 10:19:38 AM	SAVPN_LOG_EVENT	L3VPN_RemoveSiteAttachment_PE
3636	1143	fhustedand2	ActivateConfiguration	Aug 13, 2008 9:55:49 AM	SAVPN_LOG_EVENT	L3VPN_AddSiteAttachment_PE
3737	1143	fhustedand2	ActivateConfiguration	Aug 14, 2008 11:08:15 AM	SAVPN_LOG_EVENT	L3VPN_ModifyFlowPoint_StaticRoutes
3648	1145	fhustedand2	ActivateConfiguration	Aug 13, 2008 10:00:17 AM	SAVPN_LOG_EVENT	L3VPN_AddSiteAttachment_PE
3692	1145	fhustedand2	ActivateConfiguration	Aug 13, 2008 4:00:20 PM	SAVPN_LOG_EVENT	L3VPN_RemoveSiteAttachment_PE
3066	1160	fhustedand2	ActivateConfiguration	Aug 1, 2008 2:30:24 PM	SAVPN_LOG_EVENT	L2VPWS_AddSite
3070	1160	fhustedand2	ActivateConfiguration	Aug 1, 2008 2:30:24 PM	SAVPN_LOG_EVENT	L2VPWS_AddSite
3711	1161	fhustedand2	ActivateConfiguration	Aug 14, 2008 9:39:20 AM	SAVPN_LOG_EVENT	L3VPN_AddSiteAttachment_PE
3748	1164	fhustedand2	ActivateConfiguration	Aug 14, 2008 1:04:19 PM	SAVPN_LOG_EVENT	L3VPN_AddSiteAttachment_PE
3749	1164	fhustedand2	ActivateConfiguration	Aug 14, 2008 1:04:20 PM	SAVPN_LOG_EVENT	L3VPN_AddSiteAttachment_PE
3768	1169	fhustedand2	ActivateConfiguration	Aug 14, 2008 2:33:28 PM	SAVPN_LOG_EVENT	L3VPN_AddSiteAttachment_PE
3773	1169	fhustedand2	ActivateConfiguration	Aug 14, 2008 3:03:34 PM	SAVPN_LOG_EVENT	L3VPN_RemoveSiteAttachment_PE
3784	1170	fhustedand2	ActivateConfiguration	Aug 14, 2008 3:05:42 PM	SAVPN_LOG_EVENT	L3VPN_AddSiteAttachment_PE
3795	1170	fhustedand2	ActivateConfiguration	Aug 14, 2008 3:30:01 PM	SAVPN_LOG_EVENT	L3VPN_ModifyFlowPoint_QoS
3802	1170	fhustedand2	ActivateConfiguration	Aug 14, 2008 3:40:01 PM	SAVPN_LOG_EVENT	L3VPN_ModifyFlowPoint_QoS
3839	1170	fhustedand2	ActivateConfiguration	Aug 15, 2008 3:30:02 PM	SAVPN_LOG_EVENT	L3VPN_ModifyFlowPoint_QoS
3846	1170	fhustedand2	ActivateConfiguration	Aug 15, 2008 3:40:01 PM	SAVPN_LOG_EVENT	L3VPN_ModifyFlowPoint_QoS
3866	1170	fhustedand2	ActivateConfiguration	Aug 18, 2008 9:10:55 AM	SAVPN_LOG_EVENT	L3VPN_ModifyFlowPoint_QoS

Applied Filter		**Service Id:**		**Event type:** SAVPN_LOG_EVENT		**From:**		**To:**
Class:		**JobId:**		**User:**		**Workflow:**		**Step:**
Message:								

- In the above view a **Filter** selecting the **Event Types** as **SAVPN_LOG_EVENT** has been used to reduce the number of entries

- In the Audit Messages view, select the desired entry based on **Service Id**, **Date** or Service type (**Step**). This brings up the more detailed *Audit message detailed information* view

Audit message detailed information

Host name:	fhustedand2
Service Id:	1056
Order Id:	41
Type:	
State:	
Event type:	SAVPN_LOG_EVENT
Date:	Oct 16, 2009 4:38:12 PM
Class:	
JobId:	20334
User:	
Workflow name:	ActivateConfiguration
Step name:	L3VPN_AddSiteAttachment_PE
Message:	Customer:"Baldor Electric Company(22)" VPN:"Sales(1054)" Site:"Sales1 (1055)", Router id: 1, Activation Type : Add L3 Site Attachment VPN PE

Variable	Value
Router Name	C3600-1
Operator name	dk
VPN Name	Sales
Router ID	1
Workflow Name	L3VPN_AddSiteAttachment_PE
Activation Template	<?xml version="1.0" encoding="UT... Download all content
Customer ID	22
VPN ID	1054
Router Interface Id	864
Network ID	100
Service ID	1056
Region	Denmark
Router Interface	Ethernet1/0.3001
ClientIP	127.0.0.1
Service Name	Add L3 Site Attachment VPN PE
Site Name	Sales1
Activation Connect	telnet://16.49.201.237
Location	Copenhagen

Close window

- This view contains a general information section and a Variable-Value section which contains the VPN_SVP specific audit information, including the **Activation Template**.

- Select the Download all content link which allows you to view the activation template that was used when configuring the selected service. This file is xml formatted and conforming to the syntax specified by the CLIPlugin. In this format, the activation template file may be used as input to the CLIPlugin to re-configure the router exactly as was done originally.

10-6 VPN Log

The progress and result of services activated by VPN_SVP is reported in a VPN specific log available for later inspection and validation in case of failures or other issues.

To inspect the VPN log files, proceed according to the following steps:

- Log in to Service Activator.

- Select *Lobs* from the *Work Area* menu in the left navigation pane. This will open the HPSA *Logs* view.

- Locate the **SAVPN** tab to locate the VPN_SVP specific log files.

- Select **savpn_active** from the list of log files to get the most recent entries. Older log entries are rolled into numbered files over with the most recent having the highest number.

Below example illustrates an L2VPWS service activation trace as it will be seen in the SAVPN log:

The Controller workflow receives the service request 1:34:57 and instantiates the L2VPWS_CreateVPWS workflow with a service id of 1262.

This workflow instantiates the L2VPWS_AddSite workflow twice, once for aEnd and once for zEnd each of which completes OK. Finally the Controller workflow returns state OK to the order portal 1:35:24.

Logs

Host Name: fhustedand2 ▼

| CONNECTOR | MWFM | **SAVPN** | DEPENG | RESMGR | DM | SYSTEM | PM |

Hostname	Time	Component	Message	Service Id	Part	Topic	Thread
fhustedand2	Aug 26, 2008 1:34:57 PM	Controller	"L2VPWS_CreateVPWS" action "create" servicename "L2VPWS"	1262	COMPONENT		MWFM Worker 2
fhustedand2	Aug 26, 2008 1:34:57 PM	L2VPWS_CreateVPWS	Service Id: 1262 - Create L2 VPWS ENTER	1262	COMPONENT		MWFM Worker 1
fhustedand2	Aug 26, 2008 1:35:23 PM	L2VPWS_AddSite	Service Id: 1262 - Add L2 VPWS PE ENTER	1262	COMPONENT		MWFM Worker 1
fhustedand2	Aug 26, 2008 1:35:23 PM	L2VPWS_AddSite	Service Id: 1262 - Add L2 VPWS PE OK	1262	COMPONENT		MWFM Worker 3
fhustedand2	Aug 26, 2008 1:35:23 PM	L2VPWS_AddSite	Service Id: 1262 - Add L2 VPWS PE ENTER	1262	COMPONENT		MWFM Worker 5
fhustedand2	Aug 26, 2008 1:35:24 PM	L2VPWS_AddSite	Service Id: 1262 - Add L2 VPWS PE OK	1262	COMPONENT		MWFM Worker 3
fhustedand2	Aug 26, 2008 1:35:24 PM	L2VPWS_CreateVPWS	Service Id: 1262 - Create L2 VPWS OK	1262	COMPONENT		MWFM Worker 2
fhustedand2	Aug 26, 2008 1:35:24 PM	Controller	Service Id: 1262 - Status OK, Workflow "L2VPWS_CreateVPWS" action "create" servicename "L2VPWS"	1262	COMPONENT		MWFM Worker 3

savpn_active	savpn_78	savpn_77	savpn_76	savpn_75	▲
savpn_74	savpn_73	savpn_72	savpn_71	savpn_70	
savpn_69	savpn_68	savpn_67	savpn_66	savpn_65	▼

11 Back-up and Restore

11-1 Device Configuration Back-up and Restore

The VPN_SVP supports device configuration backup and restore procedures via the Backup tool described in section 3-9 . The configuration files are stored in the database of VPN_SVP.

You or the administrator can choose according to your preference the transfer protocol, TFTP or other. The NEs to be backed up must support the chosen protocol and a server or daemon version of the protocol (e.g. TFTPD) must be installed on your HPSA platform. The transfer protocol is not part of the VPN_SVP.

The interface between VPN_SVP and the transfer protocol selected is via the local file system on HPSA platform. VPN_SVP will transfer to/from the file system and from/to the database – the transfer protocol will transfer between the file system and the NEs.

The templates under $SOLUTION/etc/template_files must be customization in order to use other transfer protocol than tftp. E.g. for Cisco devices it would be Cisco/Cisco_Save_Config.xsl and Cisco/Cisco_Manual_Backup_Config.xsl that needs to be changed according to the requirements of the devices and the transfer protocol.

A backup may be initiated by the network operator (manual) or they may be made according to a predefined schedule.

The tool allows you to recover a failed PE by restoring the last saved configuration backup unto a new replacement PE router when that has been installed into the network.

The backup tool could be combined with the audit trails described above in section 10-5 to reconfigure all the services activated after the last saved configuration backup and until the point in time when the PE router failed. This functionality is not currently available.

11-2 VPN_SVP Inventory Back-up and Restore

Backup and restore of your inventory data may be made using standard database backup tools which will not be described further in this guide.

VPN_SVP provides a dedicated Inventory backup and restore feature via the XML importer/exporter tool box. You need a command line prompt/shell to execute the XMLImporter/exporter tools.

The VPN_SVP inventory data is divided in two types: the CRM Portal related data and the HPSA related data. Follow these steps to create a back-up of you HPSA based VPN_SVP Inventory data in XML format:

- Change directory to *$SOLUTION*/bin/XMLConverter
- Locate the executable Exp.sh
- Execute **./Exp.sh export.xml <output.xml>**
  where export.xml is an internal file containing the list of the database tables to be exported and <output.xml> is the file to which the exported data will be written.

Likewise, to export the CRM Portal data, follow these steps:

- Change directory to *$JBOSS_DEPLOY*/crmportal.sar/crm.war/WEB-INF/bin/XMLConverter
- Locate the executable Exp.sh

- Execute **./Exp.sh export.xml <output.xml>**
  where this script is used using the same syntax as described above.

These two operations generate two xml files each containing part of the inventory data.

When your installation has collocated the CRM portal with the HPSA server, a more user friendly script is also available, which ease the use of the above XMLImporter/exporter tool:

- Change directory to *$SOLUTION*/etc/VPNDemo/
- Locate the **exportXMLDB.sh** script
- Execute **./exportXMLDB.sh <session_name>**
  where <session_name> is used to generate the export xml file names in the **data** sub-directory

This script is taking advantage of the above two Exp.sh scripts to export both the HPSA based as well as the CRM Portal based inventory data into two xml files, i.e. data/<session_name>_crm.xml and data/<session_name>_sa_vpn.xml for the CRM Portal related data and the HPSA related data respectively.

The exported data is formatted in XML but still quite close to the database structure behind the data.

The exported data is now in a format suitable for later import. Follow these steps to import previously exported data:

- Change directory to *$SOLUTION*/etc/VPNDemo/
- Locate the **importXMLDB.sh** script
- Execute **./importXMLDB.sh <session_name>**
  where <session_name> is the id used when generating the export xml file in the **data** sub-directory

It is also possible to use individual XMLConverter.sh and doPopulateDB.sh script available for both CRM Portal and HPSA data. Before these are used, note that the existing database must be initialized to the proper state for loading of the XML based data using the initVPNDB.sh scripts. Therefore the above procedure using the importXMLDB.sh script is the simplest and the recommended way of doing the load of XML data, as all the pertinent steps are built-in.

⚠ **WARNING:** Please note, that when you import xml based data, the current content of your inventory database is reset and lost, even of the import process fails as the inventory data gets initialized before the xml data is imported. Hence it is recommended that you also export these data before importing new – be careful not to overwrite the xml files to be imported by using identical session_names!

---

12 NNMi Integration

Integration of VPN_SVP solution with NNMi brings the following benefits to the users of VPN_SVP:

- Provides equipment and topology load into VPN_SVP and ensures that both applications have the same view of the network.

- Provides the topology view to the network operator helping him to get an overview of the network, its status and to choose the correct resource for activation.

- Provides the network operator resource status to help determining cause of activation errors and inspect status of activated services.

12-1 Overview

The purpose of this section is to provide high-level details of NNMi - VPN_SVP integration use cases. Upcoming sections of this chapter provide more details on different features of the integration from a usability perspective. The complete details of required configurations for enabling different features can be found in chapter 10 of [*ADM*].

The VPN_SVP – NNMi Integration use cases can be broadly divided into two categories as follows:

- Resource Life Cycle Use Cases:
  - Dataload from NNMi to achieve activation ready network resource population.
  - NNMi GUI Launch from VPN_SVP Inventory views
- Service Life Cycle Use Cases:
  - NNMi GUI Launch from VPN_SVP Resource Selection and Error Handler views
  - Creation of VPN specific Interface Groups in NNMi – upon service creation.
  - Rediscovery of the NE involved in the service by NNMi – upon service creation.
  - Annotation of service information on the interfaces involved in service.
  - View NNMi Interface Group associated with the VPN from VPN_SVP service tree.
  - Deletion of service annotation information upon service deletion.

12-2 Dataload

The term dataload refers to the population of VPN_SVP equipment model from the network topology information discovered by NNMi.

NOTE: For dataload process overview, refer to[*ADM*].

The data extraction step extracts all those NE information from the NNMi, which are in the "scope" of dataload. The term "scope" refers to the exact set of network elements which are to be extracted.

VPN_SVP makes use of the "Data Enrichment" step to populate the VPN_SVP Equipment Model using CNRModel. Refer to section 10-2 of [*ADM*] for complete details on the pre-requisites, scope and enrichment files of dataload.

The user would be able to start dataload by launching the dataload workflow present under inventory tree CRModel/NNMi Dataload as shown below:

Figure 12-1 Starting dataload process
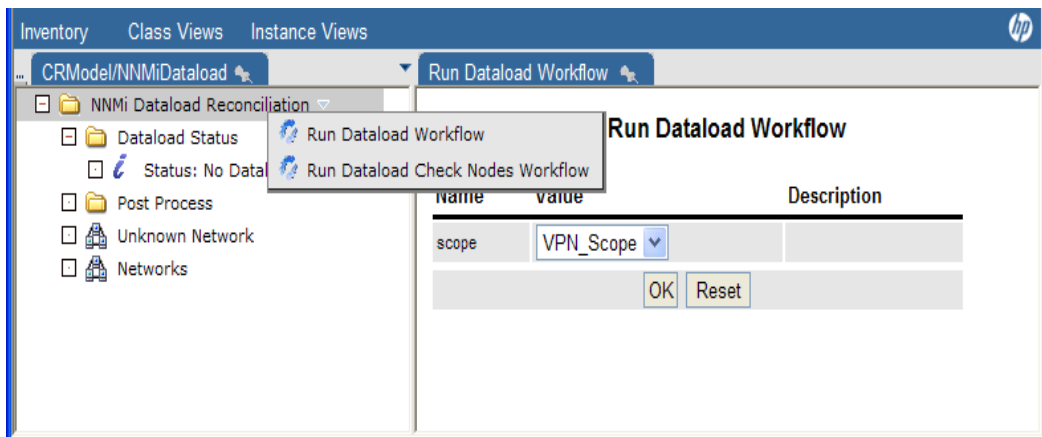
The status bar which would be displayed during the dataload processing can be used to monitor the status of dataload as shown in the figure below. Once done, there would be a visual indication of completion on the same screen – stating that, the dataload has been completed.

Figure 12-2 Dataload progress status
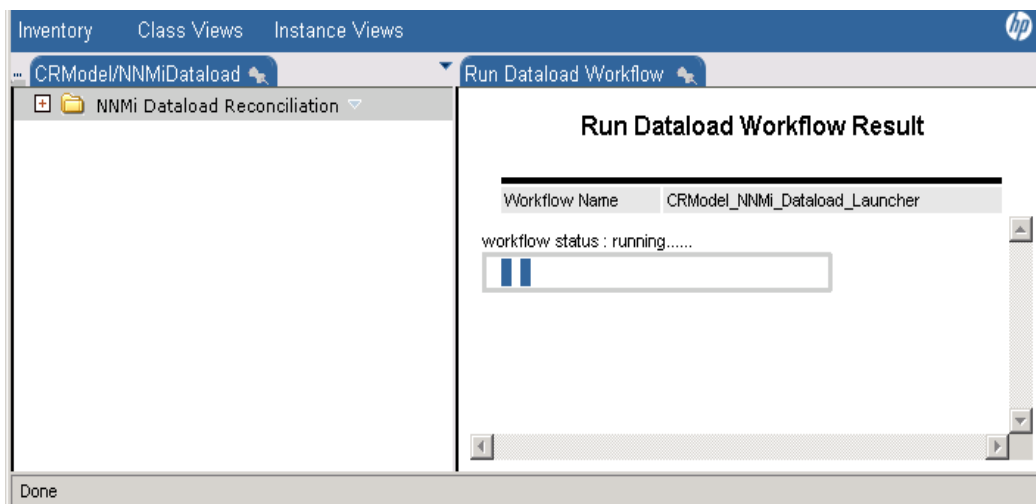
In the case of a fresh dataload with no network elements present in VPN_SVP, the network elements would be populated in the VPN_SVP inventory. The populated inventory needs a cursory examination of the different attributes being dataloaded. Once found fine, these resources can be used for service activation. In case of an incorrect value for any of the attribute, such an attribute needs to be explicitly set by doing a right-click and editing the resource.

If some of the network elements being dataloaded are already present in VPN_SVP and the dataload feature let's the operator perform a manual examination of the difference between what's present in VPN_SVP database and what's coming from NNMi. One can find all such network elements which need manual reconciliation under CRModel NNMi Dataload tree. Upon a right click on any of the network resources, the user has the option of looking at the difference between what's coming from the network and what's present in the VPN_SVP database, or the options to "Accept" or "Reject" the changes coming from NNMi.

In addition to uploading the network elements, dataload automatically performs the interface upload too. Out of the box, dataload feature executes the workflow "CRModel_PostProcess" – after processing the dataload, during "post dataload" phase. In General the administrators are advised to retain this behavior – to make the whole process automatic. In case some customizations are needed, integrators / administrators are free to configure any work-flow of their choice to be performed as a part of "post dataload phase". Find the figure below depicting this configuration – can be found under CRModel Parameters, Upload Configuration. In case the administrator prefers not to do anything after the dataload, the workflow name should be specified as empty.

Figure 12-3 CRModel_PostProces WF launch post dataload phase to perform interface upload
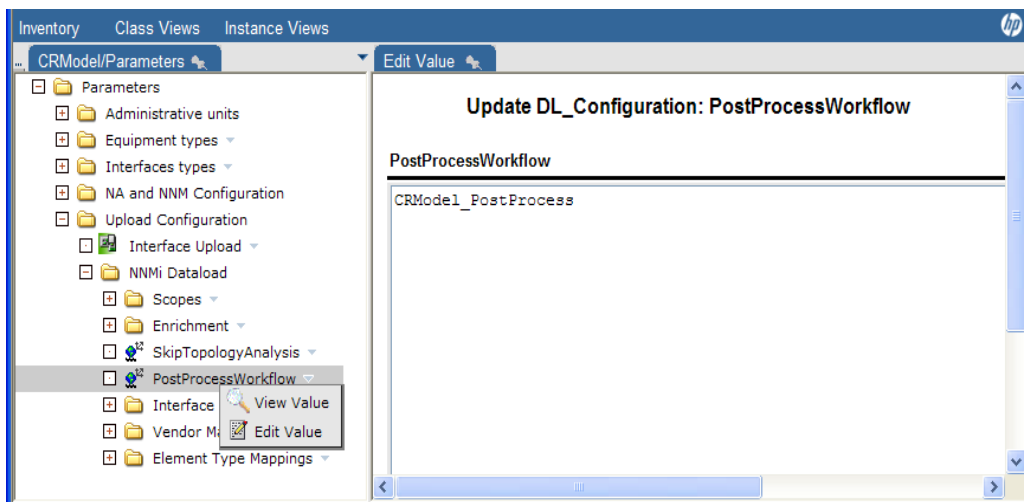
After the reconciliation and post dataload phases, the network elements are committed to VPN_SVP database – and can be used for activation. The chapters 5, 6 and 7 can be referred for more details on service activation.

NOTE: For more details on NNMi Dataload, refer to Chapter 4 of [*INTRO*].

NOTE: During dataload, only L2 connections between different network elements are dataloaded to VPN_SVP database, L3 connections would be ignored.

12-3 NNMi Views

The ability to launch NNMi views under different contexts in VPN_SVP helps the operator to make correct decisions during service creation, resource selection and trouble shooting in case of errors during service activation. Refer to section 10-1-3 of "VPN_SVP Administrator's Guide" for details on configuring this feature.

As discussed in the overview section, NNMi views can be launched under the following contexts:

● From the VPN_SVP Inventory view : Upon the right click of a network element from VPN_SVP inventory view, there are two options either to launch NNMi L2 or L3 neighbor view as shown below:

Figure 12-4 NNMi neighbor view options
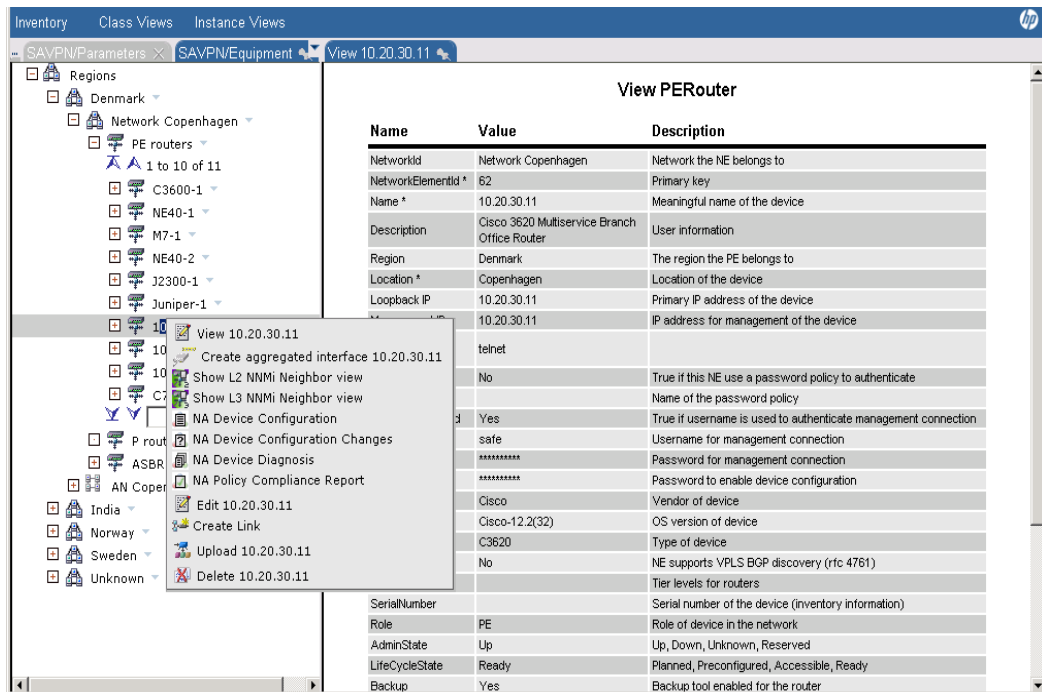
Once the view is chosen and clicked, the chosen view would be displayed from NNMi as shown below:

Figure 12-5 NNMi Neighbor view
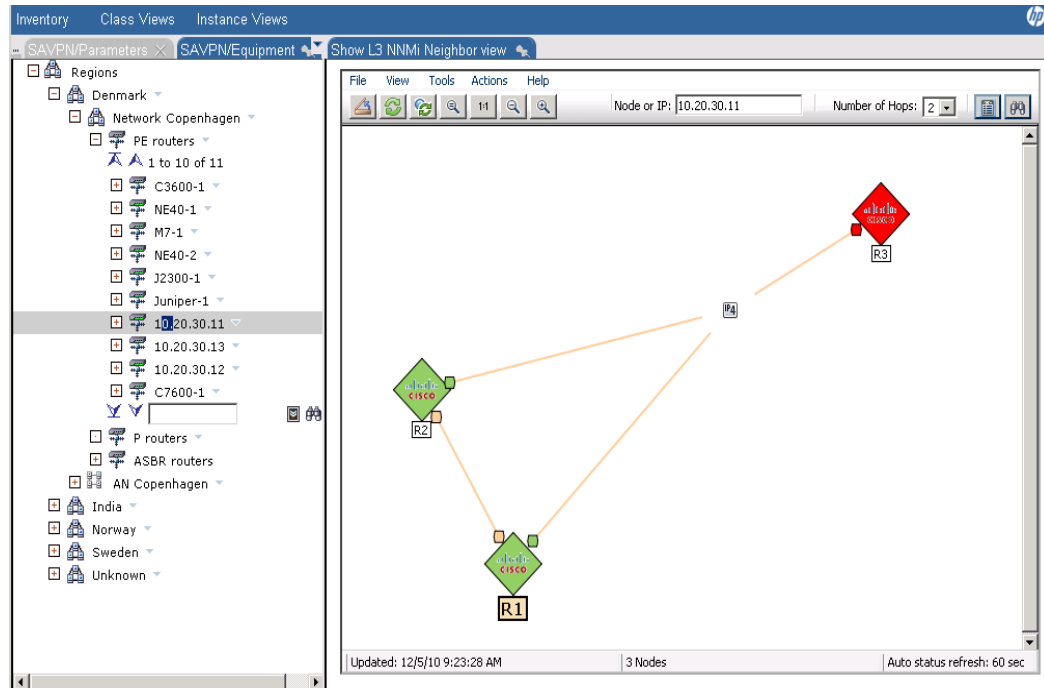
● From the VPN_SVP Resource selection page: During the service creation, in the phase where there's a need to choose the network resource to be involved in the service – in the resource selection page – the operator has the ability to launch L2/L3 neighbor views to consider the other resources, which can be used for participation in the service. Following screen shot depicts the same:

Figure 12-6 NNMi Neighbor view from Resource Selection Page

- From the VPN_SVP Error Handler: During the service creation, in case of an error and the flow could enter error-handler phase. In such situations for taking a deeper look at the root cause behind the error – the user can launch either L2 or L3 neighbor view from NNMi as shown below:

Figure 12-7 NNMi Neighbor view from Error Handler Page

12-4 Annotations

NNMi's representation of the PE interface terminating the service attachment, will automatically be annotated with service related information such as the Customer of the service, the VPN, and the associated termination point (flowpoint id) when a service is created or modified by VPN_SVP. This may help the network operator to prioritize the incidents by providing easy access to the customer and service specific information.

The annotations are made by adding the following custom attributes to NNMi's interface object:

● HPSA_Service_Type [e.g : L3VPN, L2VPN]

● HPSA_VPN_Branch_Path [Refers to the branch patch of the associated service flow point]

● HPSA_VPN_Cxy_Vabcd_Tijk [e.g. HPSA_VPN_C27_V_1038_T921]

  ○ Number followed by "C" – refers to customer ID

  ○ Number followed by "V" – refers to VPN ID

NNMi Integration

○ Number followed by "T" – refers to Flowpoint ID

● HPSA_VPN_TPid – refers to the TerminationPoint associated to the interface

The service information annotated on the interfaces can be viewed on the "Custom Attributes" tab of the interface. In order to launch this view on NNMi, perform the following steps:

● Login to NNMi

● Click on the Workspace→Network Overview →Node Form<NE>→Interfaces

● Open the interface on which service activation has happened.

● Click on the Custom Attributes tab to view the service annotations.

Figure 12-8 Service information annotation
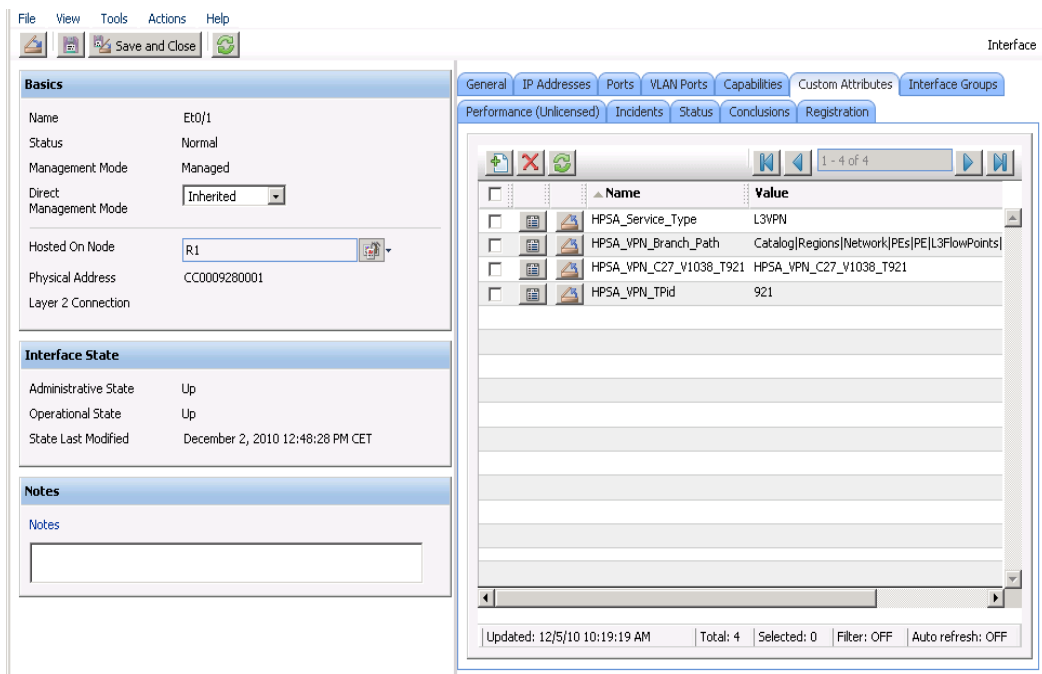
VPN_SVP

When the services are deleted from VPN_SVP, these annotations are automatically removed.

NOTE: Annotations are always created on the PE Interface.

NOTE: When Juniper logical interfaces are participating in a given service, the service annotation is done on the "Parent Interface" or the physical interface associated with the logical interface. As a consequence, during the cross launch of a flowpoint associated with a juniper logical interface, the launch always results in the display of parent interface on VPN_SVP.

12-5 Interface Group Views

The Interface Groups helps the operators to obtain a view of all the interfaces associated a specific VPN service . These custom interface groups get created upon service creation – and can be launched from VPN_SVP service tree as shown below:

Figure 12-9 Launching NNMi Interface Group View
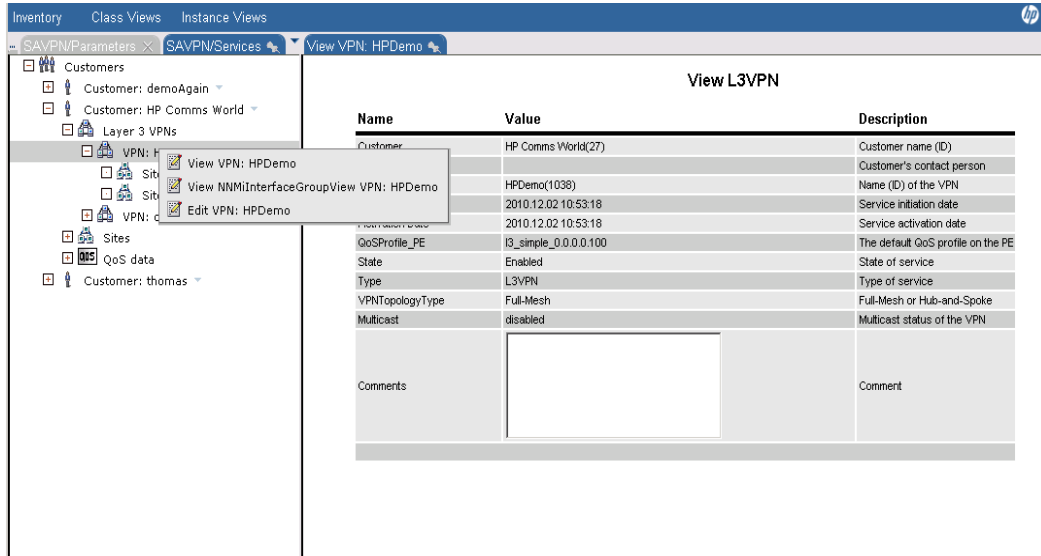
VPN_SVP operator – can easily see the status of any of the interfaces involved in a specific VPN by looking at this view:

Figure 12-10 NNMi Interface Group View
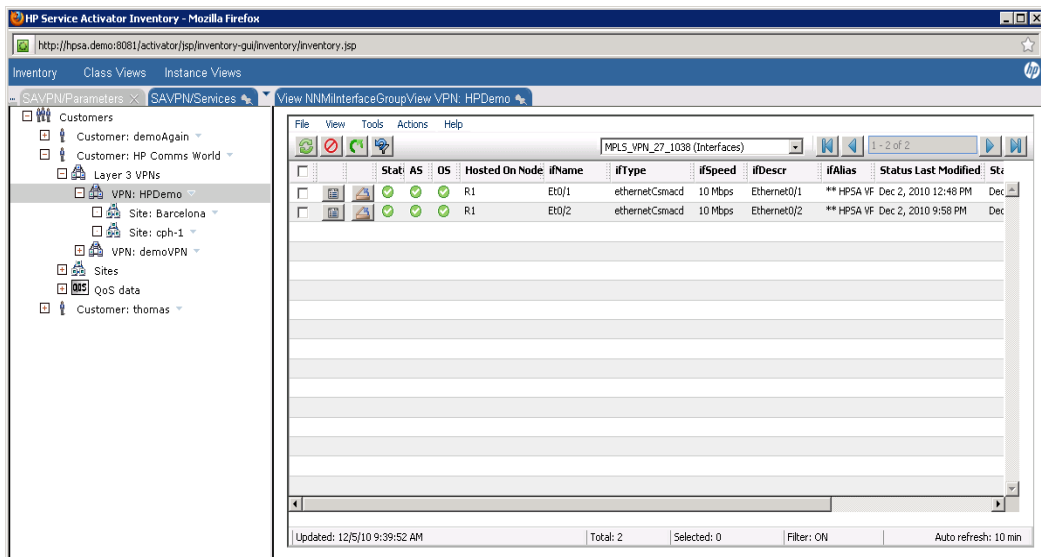
NOTE: Interfaces Groups created on NNMi - are not automatically deleted during service deletion. These need to be cleaned up manually at regular intervals. Refer to "NNMi Liaison plugin configuration" section of [*ADM*].

12-6 Flowpoint Cross Launch

Whenever an NNMi operator receives incidents on an interface, knowledge of the VPN service associated with the interface would help him decide the right priority for the incident [say when making a decision on forwarding a certain incident to the trouble ticketing system] and taking an appropriate action.

This feature provides the NNMi operator the ability to launch the VPN_SVP flowpoint view of a selected interface. Refer to section 10-1-4 in [*ADM*] for the details on configuring this feature.

The service flowpoint view can be launched from NNMi's Action->Show HPSA VPN Flowpoint View as shown below:

Figure 12-11 Launching Service Flowpoint View
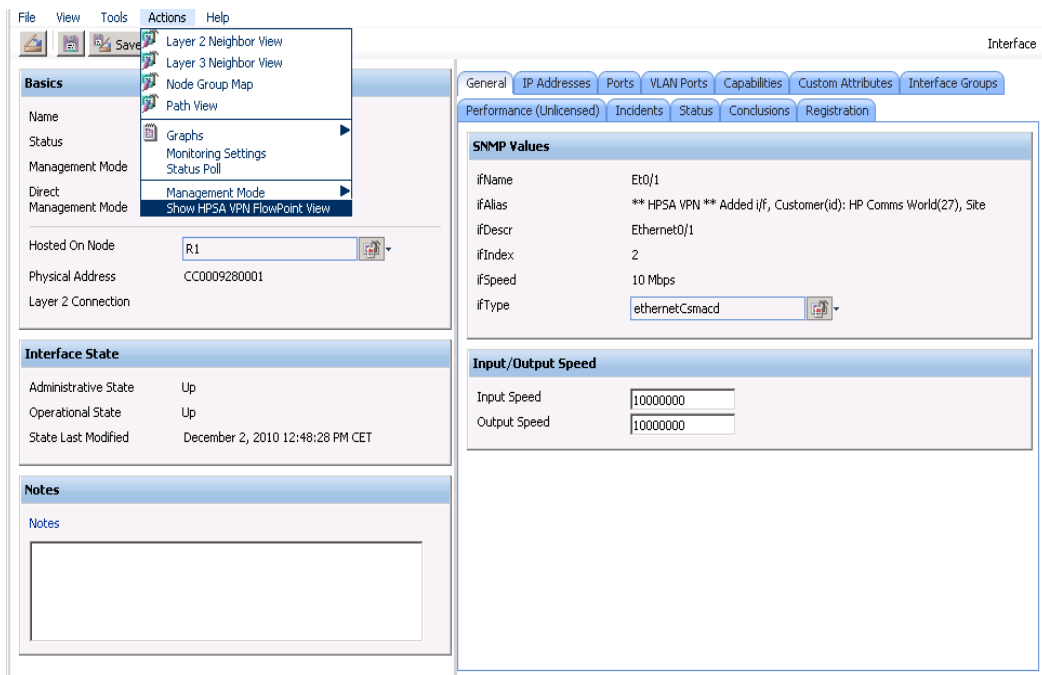
The moment cross launch option is chosen, service flowpoint view is displayed as shown below:

Figure 12-12 Service Flowpoint View

13 NA Integration

This chapter describes various NA Integration features available with VPN_SVP Solution along with the configuration life cycle to be followed to optimally utilize all the VPN_SVP→NA Integration features. VPN_SVP 5.1 provides below integration features:

- VPN_SVP→NA Cross Launch
- Service Configuration Integrity for L3VPN, L2VPN and L2VPWS services created by VPN_SVP for Cisco and Juniper Network Elements.

NOTE: You will find more information on HPSA and NA integration in Chapter 11 of.*INTEGRATE*

13-1 VPN_SVP-NA Cross Launch

The term VPN_SVP→NA Cross Launch refers to the fact of invoking and showing different views of NA from the VPN_SVP. VPN_SVP 5.1 covers following VPN_SVP→ NA Cross Launch scenarios:

- NA Device Configuration
- NA Device Configuration Changes
- NA Device Diagnosis
- NA Policy Compliance.

All the necessary parameters such as NA's protocol, hostname, port, username, password and enable CL needs to be configured before initiating Cross Launch from the Inventory GUI as shown in **Figure 13-1**. Cross launch of NA views could be disabled by un-checking the Enable NA cross Launch option.

Figure 13-1 NA Configuration for Cross Launch

13-1-1 Launching NA View's

All the users with the role "CRModel_NA_operations" are allowed to perform the NA-Related Operations including Cross Launch. All the view's for the PE's could be launch from the Equipment tree by selecting a device as shown in Figure 13-2.

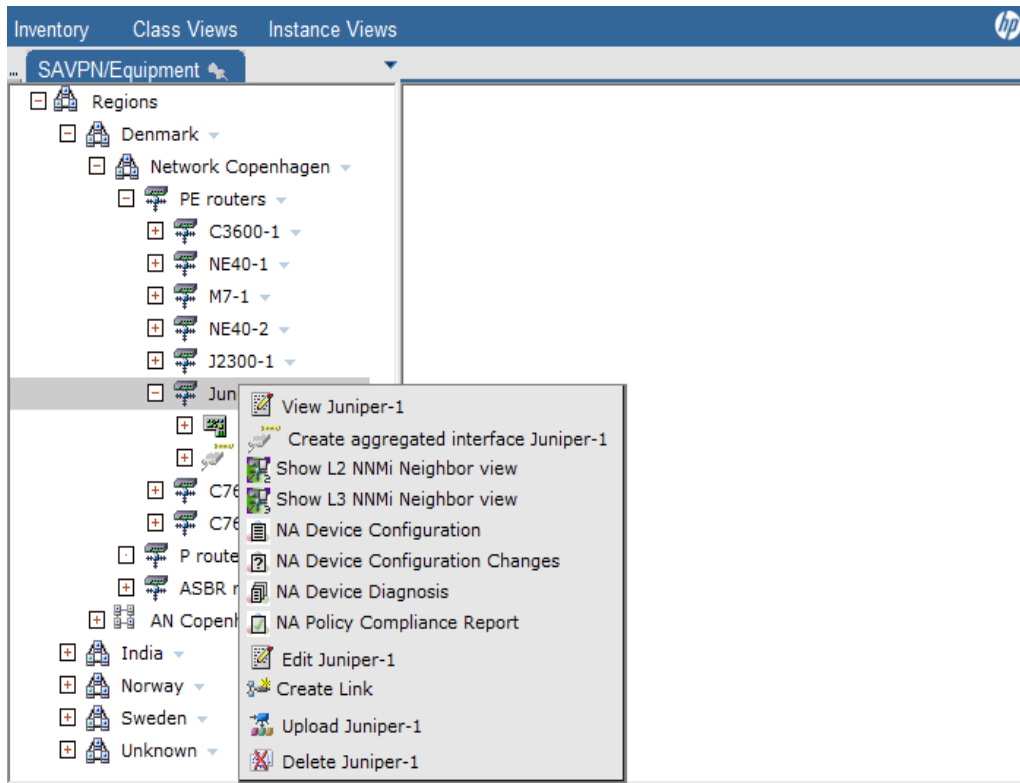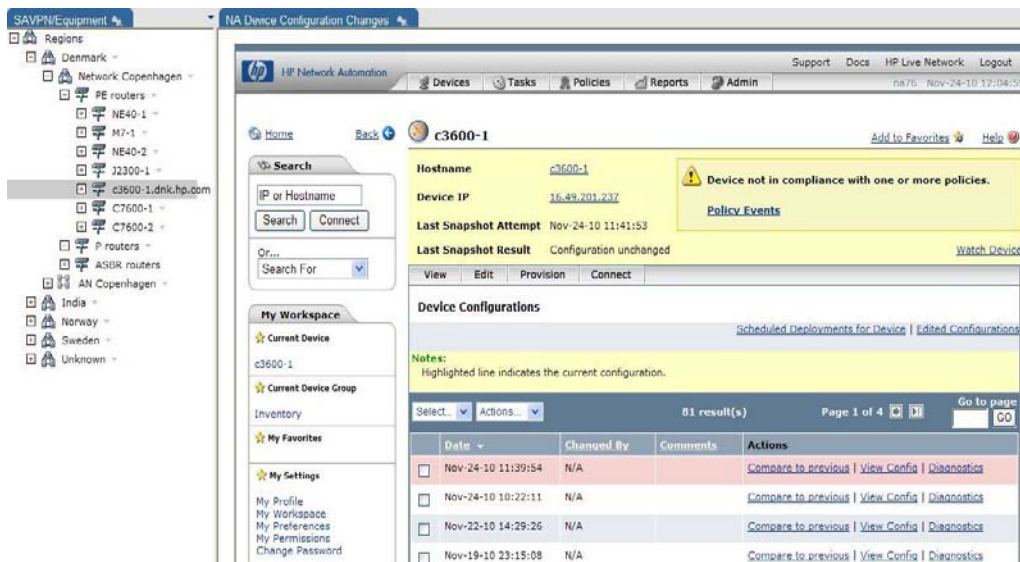**Figure 13-2** Launching NA views for the PE Router

Figure 13-3 shows the snap shot of Cross Launching the Device configuration view from VPN_SVP Equipment tree.

NOTE: To know more about the different NA view's see the [*NA_USR*].

Figure 13-3 Device Configuration View

13-2 Service Configuration Integrity

VPN_SVP solution provision and manages MPLS based L3VPN, L2VPN and L2VPWS services. However, unauthorized modification of the configuration of these service on the Network Element can create a serious security breach which will eliminate the end-users' trust to the provider's ability to manage a MPLS VPN network.

Solution like HPSA VPN_SVP deducts a successful activation based on the responses received from the device during activation. However, there is no way to check if the configuration file is in sync with the DB. VPN_SVP 5.1 addresses this limitation by using NA Service Integrity capabilities by creating Policies and associate rules to it for all the services created through VPN_SVP. See [*NA_USR*] to know more about the NA Service Integrity.

Here are the steps to be followed to add/modify or delete Policies/rules for any activation request that a HPSA received from CRM, any other northbound system or while doing Interface recovery from Inventory:

- VPN_SVP activates a service in the network.
- VPN_SVP queries the AUDIT_PARAM and AUDIT_RECORD_PARAM table to get the Activation Template file (file that contains set of commands that was executed for an activation).
- Used XSLT transformation to extract the set of extract set of <Do> commands from the set of commands.
- VPN_SVP analyze the set of <DO> commands to generate NA Policy request of addition/deletion/modification of Policies or the associated rules to it.
- Take a Snapshot of the router config after successful handling of the Policies request as mentioned in Step 4.
- Update NA_SI attribute in AUDIT_RECORD_PARAM table to reflect the status of NA policy request.

NOTE: It is assumed that Operator is not deleting an AUDIT Entry for the ongoing Activation. Configuration.

NOTE: It is also assumed that NA WF module and NA Queue is configured as mentioned in the [*ADM*].

13-2-1 L3VPN Service Integrity:

Service Integrity for L3VPN service configuration primary consists of interface and the VRF block. VPN_SVP form the below policies to monitor the L3VPN service configuration:

- Service Policy: This policy monitors the Interface bock of the L3VPN Service creation, which involve the association of QoS profile, Ratelimit, VRF, IP address to the service (interface). Service policy uses <service_id> and <ne_id> to uniquely identify it on NA. E.g. HPSA_VPN_SERVICEID_<service_id>_<ne_id>
- VRF Policy: This policy monitors the VRF bock of the L3VPN Service, which involves the associated RD, rt-import, rt-export values of the VRF. All the policies on NA requires unique name. VRF policy uses <vrf_name> and <ne_id> to uniquely form the VRF Policy name e.g. HPSA_VPN_VRF_<vrf_name>_<ne_id>

See

Figure **13-4** for the VRF and Service policies created on NA for the L3VPN.

13-2-2 L2VPN Service Integrity:

Service Integrity for L2VPN service configuration primary consists of interface and the VFI block. VPN_SVP form the below policies to monitor the L2VPN service configuration:

- Service Policy: This policy monitors the Interface block of the L3VPN Service creation, which involve the association of QoS profile, Ratelimit, vfi to the service (interface). Service policy uses <service_id> and <ne_id> to uniquely identify it on NA. E.g. HPSA_VPN_SERVICEID_<service_id>_<ne_id>
- VFI Policy: This policy monitors the VFI bock of the L2VPN Service. VFI policy uses <vfi_name> and <ne_id> to uniquely form the VFI Policy name e.g. HPSA_VPN_VFI_<vfi_name>_<ne_id>

See

Figure 13-4 for the VFI and Service policies created on NA for L2VPN.

13-2-3 L2VPWS Service Integrity:

Service Integrity for L2VPWS service configuration primary consists of interface block. VPN_SVP only form the Service Policy to monitor the QoS profile, rate limit, encapsulation to the Service:

Figure 13-4 Listing NA policies

13-2-4 Viewing Policies on NA

All the Policies that are configured on NA can be viewed by selecting Policy List under Policies menu bar. This will open the Policies page as shown in **Figure 13-4**. NA User can select following action for each policy:

- View & Edit — Opens the Edit Policy page as shown in **Figure 13-5**, where a policy can modify policies.
- Test — Opens the Test Policy page as shown in **Figure 13-6**.

NOTE: To know more about Navigating through the Policies and Rules see [*NA_USR*].

Figure 13-5 View and Edit NA Policies

13-2-5 Checking Policy Compliance on NA

All the policies that are created by VPN_SVP to monitor the Service Configuration should be validated to see if it is correctly catching issues with a device. This could be done by using the Test Policy capability of NA. NA user can choose the "Test" option as shown in **Figure 13-4**. On selecting the Test option a Test policy page will open as shown in **Figure 13-6**. When you have selected the device, click the Perform Test button to check the compliance.

NA also allows testing device configurations for the compliance against one or more configuration policies. This could be done by selecting Test Policy Compliance option under Policies menu bar. See Testing Policy Compliance section of [*NA_USR*] for more details.

Figure 13-6 Checking compliance of a policy
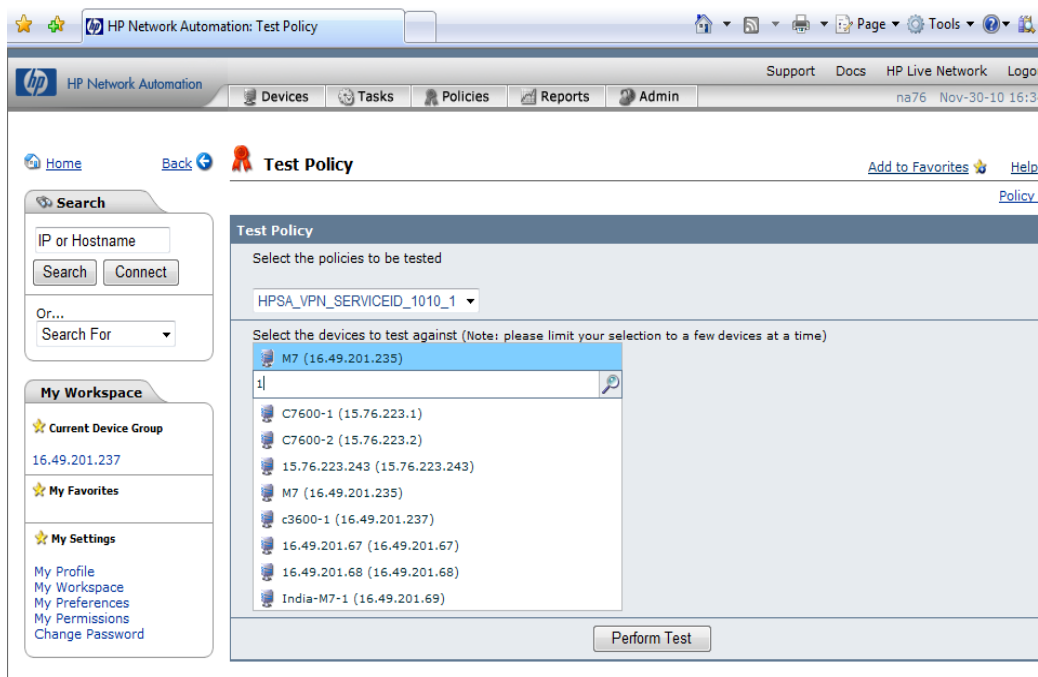
13-3 How to take Snapshot

NA provides a functionality through which an operator can check if the stored configuration in the NA database matches the running configuration on the device. If not, the task stores a new copy of the device configuration and related data in the NA database. This task on NA is termed as "Take Snapshot".

VPN_SVP also initiates "Take Snapshot" task of NA after the successful activation of service on Network Element and the creation/deletion/modification of the policies on NA. Take Snapshot task also checks the compliance of all the services that are created on the network.

To know the status of the "Take Snapshot" task, select Recent Task under the Tasks on the menu bar. **Figure 13-7** shows the status of the Take Snapshot task under the Recent Task main page of NA.

Figure 13-7 Status of the Take Snapshot task initiated by HPSA.

On selecting a Take Snapshot on NA one can see the details of the Take Snapshot task.